Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association
[2014] 1 All SA 566 (GSJ)

Division:	SOUTH GAUTENG HIGH COURT, JOHANNESBURG
Date:	19 September 2013
Case No:	2012/1249
Before:	BS SPILG J
Sourced by:	L Jantjie and T Nzimande
Summarised by:	DPC Harris

• Editor's Summary • Cases Referred to • Judgment •

[1] Delict – Defamation – Defences – Public interest and truth – Sending of bulk unsolicited advertising material via email – Electronic Communications and Transactions Act 25 of 2002 – Section 45 – Whether the section purports to set out an acceptable means of sending unsolicited advertising material and if so whether it was to be regarded as the final word on that subject – Court found that the respondent had succeeded in rebutting the inference of unlawfulness by demonstrating that the defamatory matter was true and that its publication was in the public interest.

[2] Delict – Defamation – Test for determining defamatory material is not whether specific words or conduct might bear an innocuous meaning or what the author claimed it intended to convey; rather it is whether, on a preponderance of probabilities, the ordinary or secondary meaning of the words or conduct complained of would be understood as being defamatory to the ordinary reader.

Editor's Summary

The applicant the internet to send bulk email to recipients through an independent internet service provider. The respondent was a statutorily recognised association in South Africa, of internet service providers. On the respondent's website, was a section in which it listed those whom it claimed were "spammers". The applicant sought to have its name removed from that section. It relied on the law of defamation to assert that its rights had been infringed. The respondent denied that the applicant had made out a case for defamation, but if it had, relied in substance on the defences of truth and public interest, qualified privilege and consent.

Held – In procuring the sending of bulk unsolicited advertising material via email, the applicant contended that it did so in a manner compliant with section 45 of the Electronic Communications and Transactions Act 25 of 2002. The factual question was whether the applicant had indeed complied with section 45 and the legal question was whether the section purports to set out an acceptable means of sending unsolicited advertising material and if so whether it was to be regarded as the final word on that subject.

The test for determining defamatory material is not whether specific words or conduct might bear an innocuous meaning or what the author claimed it intended to convey; rather it is whether, on a preponderance of probabilities, the ordinary or secondary meaning of the words or conduct complained of would be understood as being defamatory to the ordinary reader, even if they are capable of a non-defamatory meaning. The Court found that the listing of the applicant as a "*spammer*" in a section titled "*Hall of Shame*" on the respondent's web-page together with the overall wording of that web-page was defamatory of the applicant in its secondary meaning. It also was prepared to

accept that on the papers, the applicant's business reputation had either been affected or that at the least there was a reasonable fear that its reputation would be affected.

The Court found that the respondent had succeeded in rebutting the inference of unlawfulness by demonstrating that the defamatory matter was true and that its publication was in the public interest. The Court found no evidence that the applicant's constitutional rights were infringed.

Notes

For Delict see:

- *LAWSA* Second Edition (Vol 8(1), paras 1–171)
- *Law of Delict* (6ed) by J Neethling, JM Potgieter, PJ Visser Durban LexisNexis 2010

Cases referred to in judgment

South Africa

Borgin v De Villiers and another [1980] 2 All SA 261 (1980 (3) SA 556) (A) – **Referred to**	570
Demmers v Wyllie and others [1980] 1 All SA 391 (1980 (1) SA 835) (A) – **Referred to**	577
Dhlomo NO v Natal Newspapers (Pty) Limited and another [1989] 2 All SA 136 (1989 (1) SA 945) (A) – **Referred to**	579

GA Fichardt Ltd v The Friend Newspaper Ltd 1916 AD 1 – **Referred to** 579

Graham v Kerr (1892) 9 SC 185 – **Referred to** 571

Johnson v Rand Daily Mail 1928 AD 190 – **Referred to** 570

Marais v Richard en 'n ander 1981 (1) SA 1157 (A) – **Referred to** 570

Matthews and others v Young 1922 AD 492 – **Referred to** 579

May v Udwin 1981 (1) SA 1 (A) – **Referred to** 570

Minister of Justice v Hofmeyr [1993] 2 All SA 232 (1993 (3) SA 131) (A) – **Referred to** 579

Mohamed and another v Jassiem 1996 (1) SA 673 (AD) – **Referred to** 577

National Union of Distributive Workers v Cleghorn and Harris 1946 AD 984 – **Referred to** 577

Neethling v Du Preez and others; Neethling v The Weekly Mail and others [1994] 3 All SA 479 (1994 (1) SA 708) (A) – **Referred to** 571

Patterson v Engelenburg & Wallach's Ltd 1917 TPD 350 – **Referred to** 581

Plascon-Evans Paints Limited v Van Riebeeck Paints (Pty) Ltd [1984] 2 All SA 366 (1984 (3) SA 623) (A) – **Referred to** 579

Turner v Jockey Club of South Africa [1974] 4 All SA 52 (1974 (3) SA 633) (A) – **Referred to** 591

United States of America

Intel Corp v Hamidi Cal Rptr 3d 32 (2003) – **Referred to** 588

Omega World Travel Inc v Mummagraphics Inc 469 F 3d 348 (2006) – **Referred to** 573

Virginia State Board of Pharmacy v Virginia Citizens Consumer Council (1976) 425 US 748 – **Referred to** 588

Zimbabwe

Mahomed v Kassim [1973] 2 All SA 398 (1973 (2) SA 1) (RA) – **Referred to** 581

Judgment

SPILG J:

Nature of application

[1] The applicant ("Ketler") utilises the internet to send bulk email to recipients through an independent internet service provider. The respondent ("ISPA") is a statutorily recognised association in South Africa of internet service providers. The respondent's website contains a webpage titled "Hall of Shame" on which it lists those whom it claims are "spammers". Ketler's name appears on the list.

[2] The application was brought by Ketler to have its name removed from ISPA's Hall of Shame and to interdict its relisting. Ketler relies on the law of defamation to assert that its rights have been infringed. ISPA denies that the applicant has made out a case for defamation, but if it has, relies in substance on the defences of truth and public interest, qualified privilege and consent.

[3] The matter first came before Court on 10 April 2012. Both parties were represented and heads of argument were filed by the respective Counsel. The case was postponed at the respondent's expense in order to allow for the filing of further affidavits. On 30 April 2012, the respondent delivered a supplementary answering affidavit detailing the reasons why Ketler had been relisted on its Hall of Shame. The applicant did not respond nor did it take any further steps to pursue the application. The respondent then set the matter down for hearing on the opposed motion court roll of 12 June 2012. There was no appearance on behalf of the applicant. The respondent requested that the Court hears argument and delivers a considered judgment. I was prepared to do so but indicated that it could not be prioritised and that it would be necessary to undertake separate research.

[4] This judgment, therefore, has not the benefit of full argument. Nonetheless the respondent was brought before court and is entitled to a decision as the application was not withdrawn. It is self-evident that a party wishing to pursue the matter on the merits in the absence of the other party runs the risk of being unsuccessful. Moreover, the outcome of litigation is also of importance to a respondent which is a public interest group or association brought before court in a case involving rights issues; more particularly where it

has been obliged to incur costs and obtain legal representation to defend a position that it continues to adopt. The entitlement to a reasoned decision, whether for or against, should not be thwarted where the other party appears to have had a change of heart but has not withdrawn its application. Finally, the applicant selected the forum in which it wished to raise a right not to be defamed and since the matter has not been withdrawn the respondent is entitled to a judgment that addresses the merits of an issue which remains live between them.

[5] The disadvantage of not having the benefit of opposing argument should not necessarily inhibit providing a reasoned decision on the merits. In the present case the applicant had set out the facts and submissions that it wished to make not only in its founding and replying affidavits but also in the heads of argument filed by its Counsel. I have attempted to deal thoroughly with the issues identified in the applicant's papers and heads of argument and those which necessarily follow.

[6] The Court appears to have a discretion whether or not to provide a reasoned decision in cases where one of the parties fails to attend the hearing without withdrawing the action or defence. In my view, despite the possible diluted value of a judgment that has not benefitted from full argument on behalf of one of the parties it is nonetheless appropriate to accede to the respondent's request for a reasoned decision (compare rule 39(3) in relation to trials).

The issues

[7] The applicant contended that placing its name as a "spammer" on the respondent's Hall of Shame webpage is defamatory, that it is entitled to an order removing its name from that list and to interdict being relisted. In advancing its case the applicant argued that it has a clear right to be protected against being defamed and relied on the following submissions:

(a) Spamming is not prohibited in South Africa. Section 45 of the Electronic Communications and Transactions Act 25 of 2002 ("ECTA") allows for the transmission of unsolicited commercial communications to consumers in a regulated manner. The applicant alleges that it has complied fully with these requirements;

(b) It is not a member of the respondent's association and, therefore, not subject to the latter's code of conduct in so far as the code may allow the respondent to list spammers on its Hall of Shame. The applicant furthermore disputes that, on the facts, the respondent would have been entitled to list the applicant as a spammer even if it was an association member;

(c) Although it had signed an undertaking required by the respondent not to spam in order to enable the contracted service provider to resume the emailing of its promotional material, the undertaking is not legally binding and in any event it was withdrawn.

[8] The applicant also contended that it was not afforded an opportunity to deal with the reason for relisting and that the respondent failed to follow its own complaint procedure laid out in its Code of Conduct. The applicant added that it had no way of knowing if there were in fact any genuine complaints and, if so, whether the spam complained of occurred before or after it signed the undertaking. Although not fully fleshed out I will accept that the applicant also contended that it had a clear right, and therefore entitlement, to procedural regularity before being relisted on the applicant's Hall of Shame.

[9] In order to support the defamation claim the applicant contended that the innuendo implicit in being listed on the Hall of Shame is that it was conducting its emailing on the internet in a wrong and morally offensive manner. The consequence of the defamation is that it detrimentally affects the applicant's reputation and standing which in turn adversely impacts on its ability to generate or retain business.

[10] While the applicant did not expressly rely on an entitlement to free economic activity, I will assume that this is to be understood from its allegations that the only legitimate curtailment of its right to advertise its courses by sending bulk unsolicited emails is to be found in ECTA and that it has complied fully with the relevant provisions of that Act.

[11] Since final interdictory relief was also sought the applicant contended that there was a reasonable apprehension of harm and that it had no alternative remedy.

[12] The respondent argued that the applicant failed to make out a case of defamation, disputed that the applicant's rights were being infringed and disputed the applicant's understanding of ECTA's effect. The respondent also relied on other statutory or regulatory instruments which it averred provided consumers with additional protection and exercisable rights against spamming.

[13] The respondent conceded that it did not notify the applicant of the breaches to the undertaking but contended that it did not have to before relisting the applicant on its Hall of Shame since, on the facts, it was common cause that the applicant continued to send unsolicited mail. The respondent contended that the applicant had undertaken to desist from sending unsolicited emails and had consented to being relisted on the Hall of Shame if the undertaking was breached. It also submitted that the undertaking could not be unilaterally withdrawn.

[14] Properly analysed, the respondent has raised, aside from consent, two of the usual defences to a defamation; one of qualified privilege and the other of truth and public interest. The applicant did not raise improper motive (whether in the form of malice or otherwise) in rebuttal (see *May v Udwin* 1981 (1) SA 1 (A) at

12).

[15] In my view, the possible defence of fair comment is excluded because the respondent claims that the applicant's name was published in the admitted fashion as a statement of fact (as opposed to an opinion) that the applicant is a spammer (see *Marais v Richard en 'n ander* 1981 (1) SA 1157 (A) at 1167E–F).

[16] The respondent addressed the issue of not affording the applicant an opportunity to make representations before relisting it as a spammer on the basis that its complaint procedure only applied to members. It also contended that even if it ought to have put the allegations to the applicant and afforded a hearing, the facts were so glaring that in the circumstances the applicant's failure to explain its own documentation overcame any procedural irregularities.

[17] In an attempt to deal systematically with the issues distilled from the papers it appears advisable to:

(a) establish whether the statement constituted defamatory matter and whether the applicant has an enforceable right;

(b) determine whether the statement was true (which is relevant to the defence of truth and public interest (see *Johnson v Rand Daily Mail* 1928 AD 190 at 197);

(c) establish the respondent's status, if any, and any relevant legislation in order to satisfy:

(i) the requirement that the respondent was discharging a public duty or the exercise of a right to those who had a duty or right to receive the statement (in respect of the qualified privilege defence, see *Borgin v De Villiers and another* 1980 (3) SA 556 (A) at 577D–G [also reported at [1980] 2 All SA 261 (A) – Ed]

and *Neethling v Du Preez and others*; *Neethling v The Weekly Mail and others* 1994 (1) SA 708 (A) at 769G–H [also reported at [1994] 3 All SA 479 (A) – Ed]);

(ii) a possible factor relevant to whether publication was for the public benefit (in respect of the defence of truth and public benefit or interest, see *Graham v Kerr* (1892) 9 SC 185 at 187 and *Neethling* at 770E read with 776C);

(d) consider the applicant's right to freely impart information and ideas particularly in relation to its freedom to trade;

(e) consider whether the applicant's undertaking included a consent to have its name relisted on the Hall of Shame;

(f) Determine whether the applicant had a right to be heard before it was relisted on the Hall of Shame and what consequences flow if it was so entitled.

[18] Since the issues are relatively novel it is advisable to deal briefly with some aspects of the internet, the involvement of the internet service provider and the bulk dissemination of unsolicited advertising via emails.

Internet service providers ("ISPS") and email messaging

[19] As with most successful technological advances, products and applications that were initially the preserve of those within the industry over time become part of everyday life and the terminology or jargon used enters everyday speech. Although information technology and the use of the internet is now commonplace, it is not necessarily accessible to all. Moreover the significant role played by the internet service provider in the functioning of the internet and in particular the sending of emails may require elucidation.

[20] Without a basic understanding of the role and functioning of the internet service provider ("ISP") it would be difficult to appreciate the various rights, powers, duties and obligations which an ISP attracts. It would also be difficult to appreciate the significant role the ISP is accorded in the legislative framework of electronic communications and also the nature of the responsibilities it might ordinarily be expected to assume; a consideration relevant to the extent to which the law may allow, as opposed to oblige, an ISP to deal with issues that directly affect the interests of its subscribers and over which it may have been accorded some degree of oversight, responsibility or control.

[21] An appropriate starting point is to recognise that the internet service provider is central to the use of the internet. The ISP is the primary means whereby consumers can access the internet, whether to obtain information or for messaging.

[22] The internet, in the simplest terms, "is a worldwide network of computers all connected to each other by telephone lines, cables and satellites" (quoted from the *BBC's Beginner's Guide to the Internet*). This is consistent with the definition adopted by ECTA which is the legislation principally concerned with facilitating and regulating electronic communications and transactions. In terms of ECTA an electronic communication includes an "email" (see the definition of "email" in section 1).

[23] The internet adopts a single uniform language of transmission that allows for a global network of computers or similarly enabled devices (such as a smartphone) to communicate with each other. Communication is by means of transferring packages of digital data between internet enabled devices. The data transmitted via the internet can take a number of forms. Among the most familiar are webpages of websites and email messaging. The enormous volume of transmissions generated on the internet can be readily appreciated when it is considered that there are hundreds of millions of users who, aside from accessing information on

websites and sending emails, may also be downloading audio and video files (such as feature films and entire television series) or are communicating with each other on SKYPE and also on various social media networks.

[24] In order to use the internet, whether for purposes of sending or receiving emails, or accessing information from or interacting with websites and their webpages, it is necessary to connect the computer or similarly enabled device via an internet service provider (also referred to as a network provider). Accordingly, a user can only send or receive emails if he or she has an email account with an ISP (or utilises one of the free web accounts available on some of the major sites). Similarly the other features of the internet, including accessing websites and their pages, are only available through an ISP. In short an internet connection can only be facilitated through an internet service provider. Aside from providing internet access an ISP may also provide related services. ECTA identifies an ISP as anyone who provides "information system services", a term which is defined to include:

> ". . . the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service."

See section 70 read with section 1.

[25] An ISP provides cheap internet access to consumers who would otherwise have to incur a significant capital investment in acquiring and maintaining servers. Moreover, a local ISP may itself have an arrangement to gain access to parts of the internet beyond the home network with another "upstream" ISP (say in another country).

[26] As a consequence any email sent, whether individually or in bulk, will ordinarily have to pass through at least one internet service provider. Perhaps of equal importance is that unlike ordinary surface mail there is a cost incurred by the recipient when receiving emails; the undisputed evidence of the respondent is that it comprises the transmission cost whether in the form of internet access fees, telephone call charges or anti-spam software.

[27] Aside from creating a cost for the recipient, there is also the inconvenience of receiving unwanted emails. The inconvenience and cost is exacerbated when the consumer utilises a smartphone to access them. Modern cell phones with smartphone functionality come with standard, factory installed applications to facilitate convenient mobile email access.

In the result, the effect on consumers of receiving unsolicited promotional messages via email is not confined to computer use but impacts on the use of cell phones by effectively increasing the subscription costs of using a cell phone which is a convenient, and possibly for some the only practical, means of email messaging.

[28] Email is perhaps the most convenient means of communicating whether for work-related activities or socially. Its other attributes are low cost, mobility and speed of communication irrespective of where in the world the respective parties happen to be. In the result, unsolicited advertising material reduces the convenience of using emails and increases overall costs to the consumer. It is also significant that one of the biggest providers of email software programs, Microsoft, discourages its users from "unsubscribing" (see Microsoft's "Outlook 2007 Help" webpage on spam and junk email) as this would verify the recipient's address as being active and, as can be inferred from the papers before me, this information itself can be on-sold or used when the spammer moves to another website or adopts other means to evade anti-spam measures.

[29] However, the use of emails as a medium of communication has also opened up unique commercial opportunities. The expansion of the internet industry is regarded as benefitting the economy as a whole. The selling of clients' lists by merchants and banks is now part of daily life, irrespective of the issue whether it amounts to an impermissible invasion of privacy absent express and informed consent. Lists can also be "harvested" in other ways by those wishing to market their products or services through promotional material sent *en masse* by email.

[30] ECTA recognises both the economic and social importance of electronic communications as well as the need to promote technology neutrality in the application of legislation (sections 2(1)(a) and (f)). In so far as electronic transactions are concerned, which are distinguished from electronic communications (for example the preamble to section 2(1)), the express objects of the Act are to encourage investment and innovation in this field while at the same time promoting its development in a manner that not only is effective for consumers but responds to the needs of users and consumers (sections 2(1)(i) and (k)). In broad terms, ECTA recognises both the advantages and pitfalls of electronic communications.

In *Omega World Travel Inc v Mummagraphics Inc* 469 F 3d 348 (2006), the Fourth Circuit Court of Appeals put it as follows in the context of interpreting the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act") legislation in the United States:

> "Congress saw commercial e-mail messages as presenting both benefits and burdens. Congress found that '[t]he convenience and efficiency of electronic mail are threatened by the extreme growth in volume of unsolicited commercial electronic mail' . . ., but also that e-mails 'low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce'."

There is no reason to believe that our Legislature would not have been cognisant of these factors when considering the drafting of the electronic

communication sections of ECTA. Accordingly, certain of the objects of the Act mentioned earlier (for example

in sections 2(1)(a) and (f)) should be understood in this context.

The parties

[31] The applicant provides training courses throughout South Africa on subjects such as leadership, project management and presentation skills.

[32] The courses are marketed in a number of ways, including by means of newsletters which are sent by email. The applicant states that it:

> ". . . provides the service provider with copies of the newsletters to send out and lists of email addresses to send them to and the service provider does the actual sending (posting) of the emails."

Although the applicant does not indicate whether the lists of email recipients are created by it or are purchased or otherwise procured from other sources, the promotional material is sent to those on the list via bulk email transmissions. Naturally, the emails can only be transmitted via independent internet service providers with whom the applicant subscribes. The applicant's papers indicate that at least some ISPs it had contracted with to transmit bulk emails are members of the respondent.

[33] The respondent is a voluntary association of some 150 large, medium and small internet service providers. It represents the vast majority of ISPs in South Africa. Moreover the Minister of Communications, by notice in the *Gazette*, recognised ISPA as an industry representative to providers of information system services. The import of such recognition will be dealt with later. For present purposes, it suffices that the Minister will only recognise such an association if its members are subject to a code of conduct (see section 71(2)(a) of ECTA).

The applicant's bulk email advertising

[34] It is common cause that the applicant procures the sending of bulk unsolicited advertising material via the email. It contends that it does so in a manner compliant with section 45 of ECTA. The factual question is whether the applicant has indeed complied with section 45 and the legal question is whether the section purports to set out an acceptable means of sending unsolicited advertising material and, if so, whether it is to be regarded as the final word on that subject.

[35] The relevant portions of section 45 provide that:

> "45 (1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer –
>
> (a) with the option to cancel his or her subscription to the mailing list of that person; and
>
> (b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.
>
> (2) . . .
>
> (3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable on conviction to the penalties prescribed in section 89(1).

> (4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1)."

The penalties provided for in section 89(1) are a fine or imprisonment for a period not exceeding 12 months.

[36] The applicant's standard emailed newsletter contains details of the sender, date, recipient and subject-matter. The recipient is identified as the "Reader" which indicates that it was bulk mailed.

[37] The newsletter also explains how the recipient came to be on its mailing list, provides a disclaimer in respect of spamming and affords a means of unsubscribing. This is all contained in a separate section immediately above the actual contents of the newsletter. I will refer to it as a justification and disclaimer notice. It reads, including its highlights, as follows:

> "You are receiving this Newsletter because you are either a *past delegate*, or you may have *requested* to receive these Newsletters or you may have been *referred* to us.
>
> *WE DO NOT SUPPORT SPAM and if you have received this mail in error* or should you not wish to receive any of our newsletters at all, please *UNSUBSCRIBE* now at the link above or at the end of the Newsletter or simply reply with *UNSUBSCRIBE in the subject box*.
>
> If you would like to be kept updated with our tips on various topics, please reply to this mail with *SUBCSRIBE* in the message box."

[38] The "Unsubscribe" link appears just above these paragraphs. In addition at the end of the newsletter, which in the specimen provided is some five pages in length, the following appears:

> "This email was sent to Richard wrightrose.co.za If you do not wish to receive these newsletters in future please *Click here to Unsubscribe*.
>
> Unsubscribe Update Profile Forward Message Join KetPres."

[39] Despite a possible criticism regarding the print size it is clear that the email provides the consumer with an option to unsubscribe.

The alleged defamation

[40] The word "spam" on its own is descriptive of the method used to disseminate a particular category of emails. The *Oxford Dictionary of English* defines the noun "spam" in the present context to mean, "irrelevant or inappropriate messages sent on the Internet to a large number of newsgroups or users". As a verb it bears the meaning of sending "the same message indiscriminately to (large numbers of newsgroups or users) on the Internet". It also acknowledges the usual explanation given as to its origins:

> "The Internet sense appears to derive from a sketch by the British 'Monty Python' comedy group, set in a café in which every item on the menu includes spam" (spam being a tinned meat product that was made mainly from ham and which is an abbreviated form of "sp(iced h)am").

[41] Both parties accept the applicant's definition of "spamming", namely, "the sending of bulk unsolicited emails or the sending of bulk commercial emails", a definition which they agree is the technical definition accepted world-wide. It is, however, evident that the sense in which it is used, and

understood in the present case, relates to the bulk sending of unsolicited commercial emails. By way of comparison, section 45 covers both bulk and individual transmissions but limits itself to unsolicited commercial emails.

[42] ISPA's home page on its website contains an easily discernable box entitled the "ISPA Hall of Shame". The box serves as a hyperlink (ie a link which will open up other websites or pages) to a webpage of the same name. The webpage contains several subheadings written in bold font. The first, which is immediately below the title, is headed "South African spammers identified in this report:", followed by a numbered list of 44 names. The applicant was the fourth name appearing on the respondent's list of 3 January 2012.

[43] The applicant alleged that the respondent has shamed it by placing its name on the list as it implies that the applicant is doing something morally offensive and wrong. It claimed that this was intended to and did detrimentally affect the applicant's standing and negatively influences an individual's decision into not conducting business with it.

[44] The respondent raised two arguments: firstly, that the word "spammer" was not defamatory because of the manner whereby the respondent has defined the term on its webpage; and secondly, that the applicant made no attempt to establish either its reputation or that such reputation has been affected by the alleged defamation. They will be dealt with separately.

[45] The respondent's Hall of Shame webpage contains a number of headings including an "Introduction" with sub-headings dealing with clearly identified topics such as "What does ISPA consider to be spam", a "Disclaimer", "Contacting ISPA" and "Known Spammers" which analysis each one named in the earlier section. In order to appreciate the respondent's contentions the following relevant portions of these topics are set out (with my emphasis):

> "Introduction
>
> The Internet Service Providers' Association (ISPA), as the representative of the vast majority of ISPs in South Africa, is releasing this report to assist South African consumers to effectively manage local unsolicited bulk mail (which ISPA terms 'spam'). There is currently significant growth in the generation of local spam and while ISPA's members do their best to keep spam out of their customers' inboxes, this does come at a cost. ISPA is consolidating the experiences of its members and other trusted parties and disseminating this information *so other ISPA members*, *ISPs and email users* (*individual and corporate*) *can make similarly informed decisions on mail they wish to* receive or *allow to pass over or through their networks. The owner or operator of a network is entitled*, *both*, *morally and legally*, *to determine what traffic flows over its network*, *provided this decision is made objectively*, *in accordance with accepted Internet standards and without ulterior motives or in contravention of the principle of Internet neutrality*.
>
> What does ISPA consider to be a spam
>
> All unsolicited bulk email is spam with the following exceptions:
>
> - Mail sent by one party to another where there is already a prior relationship between the two parties and subject matter of the message(s) concerns that relationship, is not spam.
> - Mail sent by one party to another with the explicit consent of the receiving party, is not spam.

> In essence, ISPA believes that consumers should only receive bulk mail that they have requested and/or consented to receive and/or which they expect to receive as a result of an existing relationship.
>
> Disclaimer
>
> This Hall of Shame notification is based on ISPA's definition of spam as indicated above. This does not necessarily accord with the definition in the Electronic Communications and Transactions Act, nor does it imply that spam sent is unlawful or illegal, only that it and the selling of email lists is contrary to ISPA's Code of Conduct."

[46] Under the heading "Known Spammers" the respondent indicates that the position on the list is determined by the length of time the entry has been placed there and that it might change with updates, removals and re-listings. The applicant is the fourth entry on the list. The date reflected against its name, namely, 9 July 2009, indicates the date of the applicant's last listing on the Hall of Shame. Below the applicant's name the respondent records that:

> "Ketler Presentations is a spammer with multiple reports of spam from ISPA members or trusted independent sources who previously returned a signed undertaking."

[47] The test for determining defamatory material is not whether specific words or conduct might bear an

innocuous meaning or what the author claimed it intended to convey; rather it is whether, on a preponderance of probabilities, the ordinary or secondary meaning of the words or conduct complained of would be understood as being defamatory to the ordinary reader, even if they are capable of a non-defamatory meaning (see *Demmers v Wyllie and others* 1980 (1) SA 835 (A) at 848H [also reported at [1980] 1 All SA 391 (A) – Ed]). By secondary meaning is understood words which, by reason of special circumstances that are known to the recipient of the publication, acquire a defamatory meaning by reason of innuendo (for example *National Union of Distributive Workers v Cleghorn and Harris* 1946 AD 984 at 997).

[48] Words or conduct constitute defamatory matter if their imputation lowers another person in the estimation of right thinking people generally or of a particular community or group (see *Mohamed and another v Jassiem* 1996 (1) SA 673 (AD) at 702G–703A (citing Van den Heever J (at that time)), 703E–G and 707B–C).

[49] Imputations against moral character or professional competence constitute a defamation and are not limited to allegations of criminal activity; they would include for instance dishonourable conduct or statements that cause the person to be shunned and avoided (Prof Burchell considers this as illustrative whereas Prof McKerron regarded it as a criterion – see *Burchell Principles of Delict* at 166).

[50] In the present case the word "spammer" cannot be read in isolation. It is to be considered in the context in which the word appears, namely, on a list of persons who are to be "shamed" with the innuendo that such person deserves to be shamed in a list bearing the title "Hall of Shame" as a spammer by an association which itself upholds a code of conduct sanctioned by the Government. It is in this context that I am satisfied that the

Page 578 of [2014] 1 All SA 566 (GSJ)

applicant's reputation is lowered in the estimation of at least the significant category of persons who utilise the internet as a means of sending and receiving communications.

[51] There is a distinct innuendo to consumers utilising the internet that the applicant is acting in at least a morally offensive manner in the eyes of an industry oversight body by exploiting the accessibility of the internet at the consumer's expense and in so doing has also undermined the convenience and other benefits of electronic communications to the ordinary user. The term spam, spammer or spamming in the context of the overall contents of the respondent's Hall of Shame webpage may also have the connotation that the person referred to is acting in a manner invasive of, and odious to, the privacy rights of others. Since I did not hear argument on this aspect it is unnecessary to consider that possibility further.

[52] Although not argued, it is necessary to distinguish this situation from the facility afforded on the standard internet software packages which enables the subscriber to filter "junk mail" with features expressly described as "anti-spam" or which are a "protection from spam" and which are described as tools that help to "mitigate the problem of spam", the problem being described as "the flood of bulk email that can come into your inbox, most of it being junk" (see Microsoft's "Outlook 2007 Help" webpage on spam and junk emails). In these instances, "spam" is accepted as a phenomenon which the subscriber can exclude with the expedient of applications that filter-out this category of email based on settings selected by him or her. Moreover "spam" may be used in a more generic sense to describe all forms of junk mail.

[53] This judgment, regarding the defamatory nature of the applicant's listing on the respondent's Hall of Shame, should also not be construed as relevant to cases where ISPs may utilise anti-spam software or adopt spam-countermeasures, including:

(a) blocking emails based on a set of anti-spam criteria or protocols which might also include the name of the sender;

(b) internet societies or other organisations which maintain an accessible database listing spammers, without epithets.

There are two reasons: The first is that industry representative bodies such as the respondent and their members (ie ISPs) are required to conform to the Guidelines gazetted for the industry. In section 6.8 of Part 1 to the *Guidelines for Recognition of Industry Representative Bodies of Information System Providers* (GN 1283 in *GG* 29474 of 14 December 2006) ISPs are in fact required to provide anti-spam software. The provision reads as follows:

> "6.8. *Spam Protection* Members shall follow the best industry practice in providing anti-spam software to recipients of the service in order that recipients of the service can elect to minimise the amount of spam received on their email accounts."

Secondly, in my view, the word "spammer", or a derivative, does not *per se* constitute defamatory matter. It is rather the context, the epithets and the innuendos that have led to the present finding. It should also be borne in mind that anti-spam measures taken may themselves be a more aggressive response to a sender of bulk unsolicited commercial email who has

Page 579 of [2014] 1 All SA 566 (GSJ)

successfully circumvented basic anti-spam software. The respondent in its further answering affidavit likens the anti-spam measures and counter-measures to a "never-ending 'arms race' between spammers and mail server administrators". This was illustrated by the undisputed actions of the applicant which changed its domain names, its email addresses, its return-path email addresses and its mail servers while continuing to send unsolicited bulk email. Moreover, these issues would in any event be relevant in determining a truth and public interest defence.

[54] The issue of whether the applicant has demonstrated that the defamation affected its business reputation is

answered by the fact that it is a commercial enterprise which relies on its reputation to attract custom and the respondent has not gainsaid the applicant's fear that the stigma of being listed on the Hall of Shame may adversely affect its business. It is a legitimate fear bearing in mind that the applicant may find it difficult to find an ISP to distribute its emails because of the listing. While the applicant's assertions may not be backed by chapter and verse, it is assisted by the general presumption that the publication of defamatory matter results in an injury to reputation on publication and the respondent has only raised a bare denial (see Burchell (*supra*) at 169 under "Causation"). In the case of a commercial enterprise, defamation under the *actio iniuriarum* arises from loss of business reputation or status and, unlike a claim under the *actio legis Aquilia*, actual pecuniary loss is not a requirement (see *Dhlomo NO v Natal Newspapers* (*Pty*) *Limited and another* 1989 (1) SA 945 (A) at 949G–J and 952H–953C [also reported at [1989] 2 All SA 136 (A) – Ed] applying *GA Fichardt Ltd v The Friend Newspaper Ltd* 1916 AD 1 at 5–6; and generally see *Minister of Justice v Hofmeyr* 1993 (3) SA 131 (A) [also reported at [1993] 2 All SA 232 (A) – Ed] and *Matthews and others v Young* 1922 AD 492 at 503–505). In *Dhlomo*, Rabie ACJ (at the time) speaking for the Court stated at 953C that:

> "It would be wrong . . . to demand of a corporation which claims for an injury done to its reputation that it should provide proof of actual loss suffered by it, when no such proof is required of a natural person who sues for an injury done to his reputation."

[55] I, accordingly, find that listing the applicant as a "spammer" in a "Hall of Shame" on the respondent's webpage together with the overall wording of that webpage is defamatory of the applicant in its secondary meaning. I am also prepared to accept that on the papers before me the applicant's business reputation has either been affected or that at the least there is a reasonable fear that its reputation will be affected.

Truth and public benefit defence

[56] Aside from raising the applicant's consent to have its name listed should it transgress the respondent's code of conduct, the respondent pins its defences on qualified privilege and truth and public benefit. It is preferable to first consider the defence of truth and public benefit.

[57] In my view, the respondent's further answering affidavit, to which there was no response, puts it beyond dispute (on the *Plascon-Evans Paints Limited v Van Riebeeck Paints* (*Pty*) *Ltd* 1984 (3) SA 623 (A) [also reported at

[1984] 2 All SA 366 (A) – Ed] test in motion proceedings) that subsequent to the applicant's name initially being removed from the respondent's Hall of Shame webpage the applicant proceeded to send bulk unsolicited advertising emails to at least:

(a) a "spamtrap" address deliberately created as an email address but with no user. The address is specifically set up for this purpose and has no separate existence. In other words, there is no natural person who could have engaged in any activity resulting in anyone on its behalf falling into the category of persons who the applicant claimed had prompted the sending of the email to that address; namely, that someone at the email address had either been a past delegate of the applicant or had requested to receive the email or that there had been a genuine referral. A "spamtrap" is devised by system administrators with the sole purpose of detecting a sender of bulk advertising emails who objectively could not have acquired the address directly or indirectly in the manner held out by it. I am satisfied that this has been satisfactorily demonstrated on the papers;

(b) an alias email account for one or more email addresses set up for the sole purpose of soliciting public comment regarding the re-delegation of the .za country code TLD to the "*.za Domain Name Authority*". This is called a "role email account" and as with the spamtrap could not have been harvested by the applicant in any of the manners held out by it in its newsletter's justification and disclaimer notice.

[58] The respondent also presented uncontradicted evidence that several consumers had made written requests to the applicant, under section 45(1)(b) of ECTA, for the identifying particulars of the source from which the applicant had obtained the recipient's personal information. The necessary details were not provided, nor did the applicant use the opportunity of filing a further affidavit to do so. This amounts to a contravention of section 45(3) of ECTA.

[59] The respondent also produced instances where the applicant had failed to cancel the subscription of a consumer who had requested it. However, these all appear to have preceded the initial removal of the applicant's name from the Hall of Shame. They, therefore, cannot be relied upon in the present case.

[60] Accordingly, the respondent is able to show that the applicant's conduct as a spammer is "shameful" or otherwise justifies having its estimation lowered in the minds of right thinking people by reason of it:

(a) sending unsolicited emails to someone who clearly did not fit within the category of persons relied upon by the applicant in order to explain how it had obtained the recipient's address;

(b) misrepresenting how it came to obtain the subscriber's email address;

(c) failing to provide proper details of the source from which it obtained the consumer's personal information.

[61] While the first two grounds do not amount to a wrongful act under section 45 of ECTA the last one does. Nonetheless, the fact that the first two grounds do not constitute a punishable offence does not address the

question of truth of content. The respondent made it clear that it was shaming the applicant because it sent unsolicited bulk email to people without their explicit consent or where there was no prior relationship between them (and the subject-matter of the email did not concern that relationship). Without challenging the factual averments these allegations constitute the evidence before court in motion proceedings. Accordingly, the respondent has established truth of content.

[62] In my view, the respondent would also be able to establish truth of content (and public interest) by reference to the contents of the applicant's newsletter, set out earlier. On a proper analysis of its justification and disclaimer notice, the applicant accepts that it would only be proper to have included a recipient on its bulk email list if there had been some past relationship or a referral and implicitly accepts that if this was not so then the email was sent in error with the assurance that the applicant does not regard spamming (ie entirely unsolicited bulk emailing of its newsletter) as acceptable. On this basis, the applicant effectively confirms that there is some moral opprobrium attaching to sending bulk email that was unsolicited either from the recipient or by reason of a referral. Moreover on the papers before me the applicant's claim of how it came to acquire at least some of the addresses would have been untrue.

[63] The next issue is whether the publication of the defamatory statement was in the public interest or public benefit. Burchell in *The Law of Defamation in South Africa* criticised the use of the term "public benefit" as too limiting because, in *Mahomed v Kassim* 1973 (2) SA 1 (RA) at 10A–C [also reported at [1973] 2 All SA 398 (RA) – Ed], it was held that public benefit "lies in telling the public of something of which they were ignorant, but something which it was in their interest to know". In other words reinforcing something already known would not be to the public benefit, although it might be in the public interest. This debate need not concern us and even accepting the public benefit test, it is apparent that the outcome of each case remains dependent on its own surrounding circumstances (see *Patterson v Engelenburg & Wallach's Ltd* 1917 TPD 350 at 361).

[64] The public interest or benefit requirement is informed by the nature of spam and its impact on the use by consumers who utilise the internet as a means of communicating through email messaging whether on standard computers, notepads or other devices such as cell phones. Furthermore, it is informed by the impact spam has on ISPs in their relationship with their network subscribers.

It also appears to be informed by the various legislative initiatives, whether they are prescriptive and whether they expect ISPs to play a passive role in the regulation of the industry.

[65] The undisputed evidence presented by the respondent is that 80% of internet email traffic comprises spam. This adversely affects the public at large and also network providers in a number of significant ways. The subscriber or end-user is adversely affected both because the convenience of emailing as a medium to the public at large is compromised and because it increases the cost of the service. I have already dealt with the cost

element. In regard to compromising the convenience of emails as a medium, it is time consuming for the end-user to deal with spam and inhibits the use of devices, including smartphones, to download emails as a means of enhanced mobility.

[66] The ISP is also adversely affected by spam. The high volumes of spam, on the evidence presented by the respondent, result in additional infrastructural burdens and human resource costs. By way of illustration, greater central processing unit ("CPU") activity is required for email processing, scanning and delivery. Spam also affects bandwidth (ie the capacity or volume of internet data) costs per metered data and requires support desk staff to facilitate spam complaints by customers and to manage spam filters. Moreover, the respondent's papers reveal that large sums of money are spent on commercial countermeasures, although with limited success.

[67] The Court is indebted to Ms *Nieman* for the extensive collection of legal articles, mainly from the United States but also a number from South Africa, which she provided on the subject of spam. They have been of great assistance both directly and in identifying overseas' case law and thinking on the topic. I have, however, taken care to avoid relying on the factual underpinnings used to support positions taken in the articles unless they were contained as undisputed averments in the affidavits before me. By way of illustration; the respondent's affidavit presented evidence of the extremely high percentage of spam in internet email traffic but did not provide an estimate of the percentage of time used up by consumers in deleting unwanted spam, whereas many of the arguments contained in articles justifying a more vigorous approach to spamming by the Legislature and courts did. I had regard to the former evidence (ie the estimate of 80%) but not to the latter estimates as they were not placed before me in the form of real evidence, and accordingly the applicant did not have an opportunity to rebut.

[68] It is, however, clear from the affidavit evidence placed before me that the efficient functioning of the internet and its continued convenience and low cost to the consumer as well as the individual's right to privacy without having to actively take steps to secure it are all matters of public interest.

[69] By adopting a fair process of identifying spammers (truth of content has already been dealt with), the respondent, as an umbrella body of ISPs, is able to name those who send unsolicited promotional emails in order for ISPs and individual consumers to make an informed decision regarding whether the sender's emails will be filtered in order to protect the interests of the consumer set out in the preceding paragraph. These factors appear sufficient to satisfy the public benefit requirement regarding the naming of the applicant as a spammer by the respondent.

[70] It may be contended that the qualifications of the author to name and shame someone as a spammer are relevant to this leg of the enquiry. The issue need not be debated because, assuming that it is a relevant consideration, the statements defaming the applicant emanate from a source intimately concerned with the

protection and advancement of the electronic communications industry for the public benefit and in the public interest. This arises by reason of the factors set out in the following paragraphs.

Page 583 of [2014] 1 All SA 566 (GSJ)

[71] The scheme of ECTA provides not only a legislative framework, including certain statutory offences, but also establishes a self-regulatory framework for information system service providers. Service providers can form a representative body (in other legislative instruments identified as an industry representative body or IRB) which may be recognised as such by the Minister of Communications by way of notice in the *Gazette* provided, *inter alia*, membership of the body is subject to adequate criteria, members are subject to a code which provides for adequate standards of conduct and the representative body is capable of monitoring and enforcing its code of conduct adequately. This is in terms of section 71 of ECTA (as read with the definition of "service provider" in section 70).

[72] ISPA was recognised as an industry representative body under section 71(1) and the effect is two-fold:

(a) It confirms that the Minister was satisfied, under section 71(2) of the Act, that:

(i) ISPA's members are subject to a code of conduct (subsection (a)) which would have been considered by the Minister to be adequate for the purposes contemplated in subsections (c) and (d);

(ii) ISPA's membership is subject to adequate criteria (subsection (b));

(iii) ISPA's code of conduct requires continued adherence to adequate standards of conduct (subsection (c)); and

(iv) ISPA is capable of monitoring and enforcing its code of conduct adequately (subsection (d)).

(b) It also means that a service provider who is an ISPA member will be protected from liability in the circumstances identified in Chapter XI of the Act provided it remains a member of ISPA and has adopted and implemented ISPA's official code of conduct.

[73] The scheme of Chapter XI of ECTA is manifest, and the object of creating government approved representative bodies with their own codes of conduct is to establish an acceptable self-regulated industry, subject to continued government scrutiny, for the avowed purpose of providing liability protection to service providers who satisfy adequate industry entry criteria and organise themselves in a manner which subjects them to adequate codes of conduct. The establishment of the representative bodies is, therefore, not an end in itself but a means to an end, namely, liability protection for industry players who meet the requirements of sections 71(2) and 72. This is borne out by the structure of the enabling provisions to the Chapter and is reinforced by Chapter XI's heading "Limitation of Liability of Service Providers".

[74] The enabling provisions of Chapter XI then lead into the sections which identify five specific instances where an ISPA member will enjoy protection from liability (sections 73–77), include a further general exemption (section 78) and conclude with a number of provisos (section 79). It is not necessary for present purposes to deal with any of these provisions, save that they are all concerned with acts or omissions that are expressly dealt

Page 584 of [2014] 1 All SA 566 (GSJ)

with in the Act. While this at first blush may suggest that ECTA is prescriptive as to what constitutes acceptable conduct, these sections should rather be seen in the context of safe harbour defences providing indemnity to service providers, or in the language of ECTA a "limitation of liability of service providers" (see the heading to Chapter XI and the preamble to section 72).

[75] Such an interpretation gives proper effect to section 4(2) of ECTA which expressly provides that the provisions of the Act are not to be construed as:

> ". . . prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages."

This is also the understanding reflecting in the previously mentioned *Guidelines for Recognition of Industry Representative Bodies of Information System Providers* (Gazetted under GN 1283 in *GG* 29474 of 14 December 2006). It will be referred to as the "ECTA IRB Guidelines"). The Guidelines explain the following in Part 1 paragraph 1.2:

> "1.2. *Self regulation rather than legislation*
>
> The legislative approach in Chapter XI (ie; of ECTA), as is the case elsewhere in the world, is to place the emphasis for control on self-regulation by the industry rather than directly applicable legislation or government regulation and intervention."

While this is not binding, as demonstrated earlier it certainly is consistent with the intention of the Legislature as I have considered it to be expressed in the body of ECTA.

[76] The ECTA IRB Guidelines also explain in section 2 of Part 1 that they are based on the following principles:

> "2.1 *Self regulation*: It is preferred that the regulation and control of illegal or *unacceptable conduct and content* by ISPs and the recipients of their services should be exercised by the industry itself rather than the State. There should be a voluntary acceptance of this policy and these standards by the internet industry. This is in conformance with the provisions of the ECT Act" (emphasis added).

[77] Section 5 of Part 1 of the Guidelines sets out minimum requirements which include a requirement that

members of an industry representative body, such as the respondent:

(a) shall not send or promote the sending of spam and will take reasonable measures to ensure that their networks are not used by others for this purpose. Members must also provide a facility for dealing with complaints about spam originating from their networks and must react expeditiously to complaints received (at paragraphs 5.8.1–5.8.2);

(b) shall follow best industry practice in providing anti-spam software to recipients of the service in order that they can elect to minimise the amount of spam received on their email accounts (at paragraph 6.8).

[78] The respondent's code of conduct, which was accepted for the purposes of enabling the Minister to recognise it as a representative body, deals with spam in a number of sections; the most important of which for present purposes are sections 14 and 15 to be found in Part E. In their terms these sections require ISP members to take reasonable measures to

Page 585 of [2014] 1 All SA 566 (GSJ)

prevent their networks from being used to send or promote the sending of spam and to react expeditiously to complaints received regarding spam. The provisions read:

"E. Unsolicited communications ('spam')

14 ISPA members must not send or promote the sending of unsolicited bulk email and must take reasonable measures to ensure that their networks are not used by others for this purpose. ISPA members must also comply with the provisions of section 45(1) of the ECT Act, and must not send or promote the sending of unsolicited commercial communications that do not comply with the provisions of section 45(1) of the ECT Act.

15 ISPA members must provide a facility for dealing with complaints regarding unsolicited bulk email and unsolicited commercial communications that do not comply with the provisions of section 45(1) of the ECT Act originating from their networks and must react expeditiously to complaints received."

[79] The respondent as a recognised representative body under ECTA also has extended responsibilities under the Consumer Protection Act 68 of 2008 ("the CPA"). The reason is that the respondent's code applies until such time as an industry code is prescribed under the CPA to deal with matters arising from that Act.

The CPA is concerned with the protection of consumers in regard to marketing (see subparagraph (a) of the definition of "consumer" in section 1 and also the definitions of "advertisement" and "electronic communication" which include a communication transmitted by email). The following appear to be relevant for present purposes:

(a) Section 3 includes as one of the purposes, and is a policy of the Act, the promotion of fair business practices and the protection of consumers from "unconscionable, unfair, unreasonable, unjust or otherwise improper trade practices" (see subsections (c)–(d));

(b) The provisions of ECTA are to be applied concurrently with the CPA, and if it is not possible to harmonise the two then the legislation which provides the greater consumer protection prevails (see section 2(9) read with subsection (8)). Significantly the consumers' common-law rights are preserved by section 2(10);

(c) Chapter 2 of the CPA is headed "Fundamental Consumer Rights". Part B of the Chapter is headed "Consumer's right to privacy". These rights are dealt with in sections 11–12. The salient features of these sections are that:

(i) Every person has the right to privacy which includes the right to require another person to discontinue, "or in the case of an approach other than in person, to pre-emptively block any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing" (section 11(1)(b)–(c));

(ii) In order to "facilitate the realisation of each consumer's right to privacy, and to enable consumers to efficiently protect themselves" a registry is established in which a pre-emptive block may be registered (section 11(3));

Page 586 of [2014] 1 All SA 566 (GSJ)

(d) Section 82 envisages that the Minister will prescribe an industry code, on the recommendation of the National Consumer Commission, which will have the effect of regulating the interaction between or among persons conducting business within an industry.

It appears that where there is an overlapping, the code of conduct provided for in ECTA, which is an earlier enactment, is intended to serve the same purpose as contemplated in the CPA until amended or supplanted by a code prescribed pursuant to section 82 of that Act. This would also explain why the code of conduct provisions of ECTA were not subject to the consequential amendments and substitutions effected under the Schedule 1 ("Amendment of Laws") provisions read with section 121 of the CPA.

[80] The respondent is therefore a self-regulating representative body within the framework of ECTA, recognised under statute, and is entitled to prescribe an acceptable code of conduct, which it has done. Both the ECTA IRB Guidelines and ISPA's own code governing its ISP members accord it and its members the responsibility, and in the case of the respondent necessary ancillary powers as a self-regulator, to ensure that ISP networks are not used for sending, at the least, entirely unsolicited bulk commercial emails. Moreover the Protection of Personal Information Bill of 2009, if it passes into law in its present form, also addresses spam in a manner that requires some form of relationship to exist between the sender and recipient or some other adequate connection and is therefore more restrictive on spam activities than section 45 of ECTA. The Bill currently

provides as follows:

"Unsolicited electronic communications

66. (1) The processing of personal information of a data subject for the purpose of direct marketing by means of automatic calling machines, facsimile machines, SMSs or electronic mail is prohibited unless the data subject –

(a) has given his, her or its consent to the processing; or

(b) is, subject to subsection (2), a customer of the responsible party.

(2) A responsible party may only process the personal information of a data subject who is a customer of the responsible party in terms of subsection (1)(b) –

(a) if the responsible party 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 –

(i) at the time when the information was collected; and

(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.

(3) Any communication for the purpose of direct marketing must contain –

(a) details of the identity of the sender or the person on whose behalf the communication has been sent; and

Page 587 of [2014] 1 All SA 566 (GSJ)

(b) an address or other contact details to which the recipient may send a request that such communications cease."

[81] The co-existence of a self-regulatory framework in which significant responsibilities are accorded to the respondent also precludes the applicant from either contending that section 45 is proscriptive or from submitting that it cannot be in the public interest to inhibit lawful activity. On the contrary, section 4(2)(b) of ECTA recognises that requirements can be validly established in respect of the manner in which data messages will be accepted and section 2.1 of the ECTA IRB Guidelines recognises that unacceptable conduct and content can also be regulated for by an industry representative body such as the respondent.

[82] It appears that the applicant sought to adopt a line of argument similar to the one that succeeded before the Fourth Circuit Court of Appeal in *Omega World Travel*, namely, that the enabling legislation, the CAN-SPAM Act, prescribed an acceptable national standard which did not result in Omega falling within the definition of an unlawful spammer, and because this Act pre-empted the State legislation upon which Mummagraphics relied, the latter could not meet the requirement of truth of content in order to defeat a defamation suit and was accordingly found liable to pay Omega damages. In the present case, section 45 of ECTA is not prescriptive of acceptable norms in the sending of unsolicited bulk emails. As already demonstrated there co-exists alongside the legislative sanctions a separate self-regulatory regime which is expected to deal not only with unlawful activity in the sending of unsolicited bulk emails but also "unacceptable" (being the term used in the ECTA IRB Guidelines) related activities in an effective manner.

[83] In the result, the respondent has succeeded in rebutting the inference of unlawfulness by demonstrating that the defamatory matter was true and that its publication was in the public interest.

Defence of qualified privilege

[84] This defence rests in part on a finding that the defamatory matter was published in the discharge of a duty, or the exercise of a right, to others who had a duty or interest to receive it (*Borgin v De Villiers and another* 1980 (3) SA 556 (A) at 577D–G). I am reluctant to deal with this defence as it was not canvassed at all by the applicant because the respondent raised it very late and did not set out the factual grounds upon which it relied. Since I have already found one of the defences raised by the respondent to be sound, it would be inappropriate to deal with an issue which must delve with far greater detail into the nature of the respondent's rights and duties and the ancillary powers that come with the responsibilities of being a self-regulator subject to the broad principles set out in the ECTA IRB Guidelines. I, accordingly, refrain from considering this defence.

Inhibiting trade or the imparting of information

[85] I would understand from the applicant's papers, albeit faintly, that it regards the consequences of being listed as a spammer on the Hall of

Page 588 of [2014] 1 All SA 566 (GSJ)

Shame as imperilling its entitlement to disseminate commercial information via promotional material through the internet. If correct this would directly breach the protection afforded by section 16(1)(b) of the Constitution of the Republic of South Africa, 1996 ("the Constitution") in respect of the right to freedom of expression and, possibly on a purposive interpretation of section 22 read in conjunction, a transgression of the freedom of trade in an extended sense.

These provisions read:

"16 Freedom of Expression

1. Everyone has the right to freedom of expression, which includes –

(a) . . .

(b) Freedom to receive or impart information or ideas;

22 Freedom of trade, occupation and profession

Every citizen has the right to choose their trade, occupation or profession freely. The practice of a trade, occupation or profession may be regulated by law."

[86] In *Virginia State Board of Pharmacy v Virginia Citizens Consumer Council* (1976) 425 US 748, the constitutional right to disseminate commercial information by means of advertising was recognised by the United States Supreme Court as an extension of the protection afforded by the First Amendment. This would fit comfortably within the scope of section 16(1)(b) of our Constitution. The US Supreme Court also held that advertising serves an important public purpose by ensuring a free flow of information vital to the efficient allocation of resources in the market.

[87] However, there are also countervailing constitutional rights that need to be considered; in particular the rights to privacy (section 14) and to property (section 25). I comprehend the right to privacy to include the right not have one's personal information utilised by others, whether for financial gain or otherwise, without obtaining some acceptable form of consent. The right to property may possibly be transgressed if it creates an involuntary cost for the consumer when a spam message is sent. In so far as trespass is concerned the Californian Supreme Court on appeal upset a series of earlier decisions by holding that reliance on this ground may have chilling effect on internet activity (see *Intel Corp v Hamidi* Cal Rptr 3d 32 (2003)) (compare the cases referred to in *The Law of the Internet in South Africa* edited by Reinhardt Buys (Chapter 13 paragraph 4.1.2)).

[88] I have already dealt with the direct and indirect cost of spam based on the evidence contained in the affidavits before me. Reference may be had to the alleged broader costs to the consumer and ISPs, against there being no cost (or a relatively insignificant cost) to the spammer, mentioned in articles such as "The Regulation of Unsolicited Commercial Communications (SPAM): Is the Opt-Out Mechanism Effective" by Sebo Tladi (2008 *SALJ* (125) 178 at 183–184 and "The Truth About Spam" by Shumani Gereda (September 2003 *De Rebus* 36 (426) at 51–52).

[89] I should add that the applicant sought to draw the analogy that it functions much like a marketing company that prints brochures which are disseminated through the post to unsolicited recipients. On the evidence before me, this is not so because in the case of surface mail the recipient incurs no cost and suffers no real inconvenience. Moreover, the risk of

proliferation would undermine the benefits of a messaging platform that is intended to be low cost, efficient, convenient and accessible not only on a standard computer but also on a cell phone, such risk being exacerbated because of the low or non-existent transmission costs to the sender of bulk commercial email on the internet.

[90] In my view, it is unnecessary to weigh the competing constitutional rights because the applicant has failed to set out any factual basis upon which the actions of the respondent have affected its ability to advertise. The applicant does not suggest that the respondent has prevented it from utilising the internet in any other equally efficient and lawful manner to disseminate its emails, and it has not suggested that either the governing laws (including section 45 which I have found it has contravened in one respect) or the manner adopted pursuant to the self-regulatory guidelines and framework are themselves unconstitutional. On the contrary, the respondent set out in its affidavit the alternative methods that are open to the applicant to send bulk commercial email. These methods would include sending email to previous delegates, to those who subscribe or legitimate referrals and in addition to subscribing to the Direct Marketing Association's National Opt-In list (being persons who have expressly opted to receive marketing emails from DMA members) as well as other avenues of acceptable digital marketing.

Moreover, the applicant did not produce evidence to demonstrate any adverse cost implications if it adopted the methods advocated by the respondent nor indicate any adverse impact on the reach of its advertising. Presumably in order to do so it would have to disclose the source of its lists, an exercise that would reveal how addresses were acquired or harvested and their cost.

[91] I am therefore unable to find, on the evidence presented before me, that the applicant's constitutional rights have been infringed. This also makes it unnecessary to consider whether the method adopted by the respondent to address spammers is reasonable and justifiable in the manner contemplated by the section 36 constitutional limitation provisions.

Consent

[92] Consent or *volenti non fit iniuria* requires the person to have consented to at least the intentional infliction of harm and requires some investigation into the defamed person's state of mind at the time the consent was given. Consent is absent if it was induced by fraud, force or other forms of pressure. The circumstances of the consent must also be recognised in law (see generally Burchell *The Law of Defamation in South Africa* at 260–265).

[93] In the present case, the respondent must rely on the terms of the written undertaking given by the applicant to constitute consent.

The written undertaking provides:

> "We undertake to ensure that we have properly obtained the direct or indirect consent of any consumer (including business) to which we send commercial mail, whether on our own behalf or by arrangement with a third party.

> We acknowledge that we will be removed from the ISPA Hall of Shame on the basis of this Undertaking, and that a failure to honour the terms of this Undertaking may lead to us being re-listed for a minimum further period of three (3) years."

[94] The applicant explained that the undertaking was given when its name was again listed on the respondent's Hall of Shame in 2009. This would have been on 9 July. Mr Ketler of the applicant enquired on 22 July from the respondent as to how its name could be removed. The respondent informed him that an undertaking would have to be given that the applicant would not again send unsolicited bulk emails. The applicant then signed the undertaking on 23 July 2009 on the basis that its name would be removed and this was accepted by the respondent which then attended to the removal.

[95] The applicant does not contend that it was pressurised to sign the undertaking; only that Mr Ketler had not taken legal advice at the time and was therefore unaware of other recourses available to it, although Mr Ketler does not explain what they were. He, however, claims to have been desperate to have the applicant's name removed from the Hall of Shame.

[96] The applicant claims that it subsequently revoked the undertaking because the respondent refused to provide it with details of the complaints which resulted in the applicant's name being relisted on 13 April 2010 as a spammer on the Hall of Shame .The applicant does not rely on duress but rather on not being sufficiently informed of the remedies available in a case where it believed that it had been wrongly listed.

[97] It is difficult to follow the applicant's contentions. The applicant did not seriously challenge that it sent spam prior to giving the undertaking and the Court has found that it did send unsolicited bulk emails after the initial removal of its name. There is, therefore, nothing before me to demonstrate that the applicant did not spam prior to the undertaking. It follows that the applicant provided the undertaking because of genuine complaints of spamming. The only submission left is that the applicant failed to first obtain legal advice before signing. The applicant does not suggest that it was precluded from doing so. It certainly had sufficient time to reflect on the steps it wished to take after it was listed and before electing to sign the undertaking.

[98] In my view, the consent is good and its purported withdrawal only after the defamatory matter was published is irrelevant; it would only be relevant if the withdrawal preceded the defamation. As long as the consent remained extant, the respondent was entitled to rely on it in order to relist the applicant's name.

Right to be heard

[99] The applicant also contended that irrespective of its undertaking, the respondent could only relist the applicant on its Hall of Shame provided the applicant was first afforded an opportunity to be heard.

[100] The right to be heard is not confined to administrative action taken by an organ of State. The law reports are replete with cases where a right to be heard was accorded to the member of a jockey club or a member of a

church synod, based on a submission to the disciplinary codes of a voluntary association (for example *Turner v Jockey Club of South Africa* 1974 (3) SA 633 (A) [also reported at [1974] 4 All SA 52 (A) – Ed]).

[101] A person generally has a right to be heard when his or her rights or interests may be prejudicially affected by the decision to be taken whether administratively or where the right to do so arises from a special relationship established between them as determined under law.

[102] In the present case, the respondent has acted pursuant to a power accorded to it to self-regulate an industry and the ancillary rights that come with it. While ISPs are members and if they were to be disciplined *prima facie* the right of *audi* would be accorded to them, in relation to the applicant, however, the only link is a bilateral agreement and possibly the consequences of being a self-regulatory body.

[103] Once again it is unnecessary to finally determine this point because even if it was entitled to a hearing *before* the relisting, the applicant chose the courts as the forum to demonstrate that it did not spam. The applicant failed. I do not believe that this is the type of case where a procedural irregularity vitiates the initial decision irrespective of its correctness, particularly where a full right of *audi* would allow a spammer to continue sending unsolicited bulk email indefinitely until the final resolution of the dispute (which would include rights of review and appeal before a court), whereas making representations after the relisting, either to have its name again removed or in respect of the duration of the listing, may cause little or no prejudice. Without deciding, it might be argued that in view of the self-regulatory nature of the industry and the limited potential prejudice of being listed for a short time (the advertisements could then still go to the same addresses and it is not suggested that the same courses on offer are repeated by the same candidate), the spammer ought to bear the responsibility of approaching the respondent to demonstrate that it did not spam. The issue, however, may require far greater consideration.

[104] I, therefore, remain satisfied that the respondent is not precluded from relying on the undertaking given as a consent to relist the applicant on its Hall of Shame. This remains so even if the respondent was obliged to afford the applicant an opportunity to address the subsequent complaints of spamming and even if the respondent failed to respond to a request for information. The risk run by the respondent was that it might not have been able to demonstrate an infraction of the undertaking and become liable in damages.

Order

[105] It is for these reasons that I dismissed the application with costs on 6 June 2013.

For the applicant:

Original heads of argument by *R Stevenson* instructed by *Wright Rose-Innes Incorporated*

For the respondent:

A Nieman instructed by *Dingley Attorneys*