No. A142444

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
FIRST APPELLATE DISTRICT
DIVISION FIVE

TIMOTHY A. DeWITT,

Plaintiff and Appellant,

v.

DEVRY UNIVERSITY, INC. *et al*,

Defendants and Respondents.

[PROPOSED] AMICUS CURIAE BRIEF OF THE COALITION AGAINST UNSOLICITED COMMERCIAL EMAIL (CAUCE), *ET AL.*, IN SUPPORT OF AND AGAINST ALL PARTIES

Appeal from Judgment Following Order Granting Summary Judgment in
the Superior Court of the State of California,
County of Alameda, No. RG 12638207
Hon. Ronni MacLaren

Timothy J. Walton (State Bar No. 184292)
Jim C. Twu (State Bar No. 175032)
WALTON TWU LLP
9515 Soquel Drive Suite #207
Aptos, CA 95003
Phone: (831) 685-9800
Fax: (650) 618-8687

CERTIFICATE OF INTERESTED ENTITIES OR PERSONS

Pursuant to California Rule of Court 8.208, I know of no entity or person – other than the Parties themselves – that has a financial or other interest in the outcome of the proceeding that the Justices should consider in determining whether to disqualify themselves.

Dated: April 8, 2015

/s/ Timothy Walton
Timothy Walton
Attorney for *Amicus Curiae* CAUCE *et al*

TABLE OF CONTENTS

Page

TABLE OF CONTENTS (cont.)

Page

TABLE OF AUTHORITIES

Page

TABLE OF AUTHORITIES (cont.)

Page

I.
INTRODUCTION

Amicus curiae CAUCE, *et al*[1] (collectively "CAUCE"), agree with Respondent DeVry University Inc. *et al*'s (collectively "DeVry") first statement in their Opposition Brief:

> Commercial emails that enable their recipients to identify who is advertised in the emails without opening them do not violate Business and Professions Code section 17529.5(a)(2).

Here, the From Display-Names[2] of the emails identified the advertisers and were sufficient for the average consumer to determine who the emails were from, without opening the emails. The emails at issue in this appeal are examples of truthful advertising permitted under California Business & Professions Code § 17529.5 ("Section 17529.5").[3]

CAUCE submits this amicus brief to argue that the inverse of Respondents' opening statement should also be the law: Commercial emails that do *not* enable recipients to identify the advertiser or the sender without opening them violate Section 17529.5(a)(2). More precisely, From

---

[1] *Amicus Curiae* filing this brief are: the Coalition Against Unsolicited Commercial Email ("CAUCE"), Justia, Inc., David Crocker, William Silverstein, and Lloyd Stevens.

[2] This Brief uses the term "From Display-Name" to be consistent with Request for Comment 5322, originally authored by David Crocker. The "From Display-Name" is also sometimes referred to (by others) as the "From Name," "Display Name," "Quoted From Name," and "Friendly From Name." Appellant refers to the From Display-Name as "lead header position." Respondents refer to the From Display-Name as "email header line," but this Brief will refer to that item as "From Display-Name". If an email's From Field says: "John Doe <johndoe@yahoo.com>" then the "From Display-Name" is "John Doe."

[3] All references to Section 17529 or its subsections refer to California Business & Professions Code §17529 *et seq.*

Display-Names that do not truthfully identify either the advertiser or the sender of commercial emails violate Section 17529.5(a)(2). Otherwise, California law would permit the use of deceptive and misleading tactics to trick or entice consumers to open commercial emails. Opening spam[4] can expose an email recipient to Trojan horses, computer viruses, malware, and web bugs that can cause the recipient to receive even more Trojan horses, computer viruses, malware, and spam. For this reason, this Court should reject the holding in the recently decided case of *Rosolowski v. Guthy-Renker LLC* (2nd App.Dist. 2014) 230 Cal. App. 4th 1403, 1404 which held that

> A header line in a commercial email advertisement does not misrepresent the identity of the sender merely because it does not identify the official name of the entity which sent the email, or merely because it does not identify an entity whose domain name is traceable from an online database, provided the sender's identity is readily ascertainable from the body of the email.

CAUCE also submits this amicus brief to reiterate the proper approach to interpreting and applying Section 17529.5. Section 17529.5 is part of California Business & Professions Code Section 17529 ("Section 17529"), which prohibits *all* unsolicited commercial email to and from California email addresses. Section 17529.2(a-b). Thus, courts should construe all sections of Section 17529, including 17529.5 as broadly as possible in light of this stated statutory purpose.

The only limit on this broad construction is the federal CAN-SPAM Act, 15 U.S.C. §§ 7701 et seq., which preempts state laws that expressly regulate commercial emails, except to the extent that any state statute prohibits falsity or deception in the email. *Id*. at § 7707(b)(1). By

[4] "Spam", "spams" or "UCE" mean "unsolicited commercial email advertisements."

definition, commercial email that is materially false and deceptive under CAN-SPAM is not preempted and should also violate Section 17529.5.

Under the proper approach to construing Section 17529.5, this Court should affirm the ruling of the trial court below but reject the holding of the Second Appellate District in *Rosolowski v. Guthy-Renker LLC* (2nd App.Dist. 2014) 230 Cal. App. 4th 1403 and provide lower courts with the correct analytical framework for construing and applying Section 17529.5.

II.
THE EMAILS COMPLY WITH SECTION 17529.5

A. From Display-Names That Truthfully Identify Either the Advertiser or the Sender Do Not Violate Section 17529.5(a)(2)

All Parties tacitly agree that the From Display-Name component in the From field[5] of an email is itself part of the email header information under Section 17529.5.[6] And, in order for the Summary Judgment below to stand, the From Display-Name must be distinct from the sending email address and the sending domain name. For the bulk of the emails at issue in this appeal, the From Display-Name identified the advertiser rather than the sender. Respondents do not contest Appellant's allegation that the sending domains were not readily traceable to the senders because they contend that the From Display-Names alone are sufficient to identify the advertisers.

---

[5] An example of a From Field, also referred to (incorrectly) as the "From Line," appears on the first page of attachment A to Respondents' brief: "Devry University <DeVry@erumolz.com>." The "From Display-Name" is "Devry University" and the sending email address is "DeVry@erumolz.com." The sending domain is "erumolz.com."

[6] Contrary to Respondents' assertion, the California Supreme Court noted that the California legislature *rejected* the CAN-SPAM definition of header information. *Kleffman v. Vonage Holdings Corp*. (2010) 49 Cal. 4th 334, 340 n.5

What is lost in the Parties' arguments is *why* truthful From Display-Names do not violate Section 17529.5(a)(2). From Display-Names, along with Subject Lines, are two of the few parts of an email header that an average consumer can see in an email inbox before opening an email.[7]

It is also an important factor in whether an email recipient opens an email. *See* eMarketer, E-Mail Open Rates Hinge on 'Subject' Line, *available at* http://www.emarketer.com/Article/E-Mail-Open-Rates-Hinge-on-Subject-Line/1005550 (Oct. 31, 2007)(stating that "The e-mail's 'from' and 'subject' lines become key elements that help recipients quickly decide whether the e-mail is spam," said David Hallerman, senior analyst at eMarketer) (last visited April 7, 2015). Truthful From Display-Names tell the recipient who the email is from, which is the purpose of the From Display-Name. "The From Field specifies the author(s) of the message. That is the mailbox(es) of the person(s) or system(s) responsible for the writing of the message." RFC 5322 at ¶ 3.6.2.[8]

Thus, a commercial email with a truthful From Display-Name is sufficient to inform the recipient before opening it: (1) that the email is commercial in nature; and (2) whether the recipient has already provided

---

[7] Should the Court request a citation for this fact, the amicus parties can supplement the record as Mr. Crocker is the author of the original Internet Mail specification format. Otherwise, the amici invite the Court to view an email inbox in any one of the major web based email providers: Hotmail/Outlook, Gmail, Yahoo! Mail, etc.

[8] Request for Comments (RFC) is a publication of the Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet. RFC 5322 is the definition of email headers so that email will function on the internet. *ZooBuh, Inc. v. Better Broadcasting, LLC* (D. Utah May 31, 2013) No. 2:11-cv-00516-DN *7 n. 29 (referring to RFC 2822, which RFC 5322 replaced.)

"direct consent"[9] to receive commercial email from that advertiser or sender. Whether a consumer can trace the email sender via the WHOIS database is of less import because the average email recipient is not familiar with the WHOIS database.[10]

Here, the Appellant admitted he knew who was advertising in most of the emails without opening them. (7 RA 1629-31; 7 RA 1662-63; 7 RA 1669-70; 7 RA 1691). So, he knew before opening any of the emails at issue that they were commercial emails and whether he had already provided direct consent to receive commercial emails from the advertiser.

These emails are similar to the one email from "eHarmony" in *Balsam, v. Trancos Inc. et al* (1st Dist. 2012) 203 Cal. App. 4th 1083, 1093, *petition for review denied* (Cal. May 23, 2012) 2012 Cal. LEXIS 4979, *petition for certiorari denied* (U.S. Oct. 29, 2012) 2012 U.S. LEXIS 8423, *petition for rehearing denied* (U.S. Jan. 7, 2013) 2013 U.S. LEXIS 243 – the only spam in that case that did *not* contain generic text in the From Display-Name, and the only spam for which the court did not award liquidated damages. The trial court ruled, and the court of appeal affirmed, that generic From Display-Names "Paid Survey," "Your Business," "Christian Dating," "Your Promotion," "Bank Wire Transfer Available," "Dating Generic," and "Join Elite" violated Section 17529.5, but the From Name "eHarmony" did not violate the statute because eHarmony was the name of the advertiser which is well known by the typical recipient. *Id*. at

---

[9] "'Direct consent' means that the recipient has expressly consented to receive e-mail advertisements from the advertiser, either in response to a clear and conspicuous request for the consent or at the recipient's own initiative." Bus. & Prof. Code § 17529.1(d).

[10] Technically, WHOIS is not the database itself but a protocol for submitting a query to a database in order to find contact information for the owner of a domain name. *Solid Host NL v. NameCheap*, 652 F. Supp. 2d 1092, 1095 n.3.

1093. The court of appeal affirmed the trial court in all respects. *Id.* at 1111.

B. <u>Truthful Statements in the Body of an Email Cannot Cure Deception or Misrepresentations in the Header Information</u>

Respondents cite *Rosolowskiv. Guthy-Renker* LLC (2nd App.Dist. 2014) 230 Cal. App. 4th 1403 1404, for the proposition that truthful information in the body of an email can cure any deception in the header information. (Respondents' Br. *passim*.) However, this Court should reject *Rosolowski* because it sanctions the very tactics spammers use to trick and deceive email recipients into opening email and causing the very harm that Section 17529 was designed to prevent.

Under *Rosowlowski,*

> A header line in a commercial email advertisement does not misrepresent the identity of the sender merely because it does not identify the official name of the entity which sent the email, or merely because it does not identify an entity whose domain name is traceable from an online database, provided the sender's identity is readily ascertainable from the body of the email.

Id. The practical import of this holding is that the headers can be false so long as the body discloses the senderor the advertiser. Therefore, an email that advertises sexually explicit material in the body would not violate Section 17529.5(a)(2) under *Rosolowski* even if the From Name falsely stated it came from a family member or friend of the recipient.

In order to see the body of an email, a recipient needs to open it. Opening unfamiliar email can expose the recipient to numerous harms. California appellate courts have previously rejected the idea that recipients should have to open email. In *Ferguson v. Friendfinders, Inc*., the court noted that:

> [Unsolicited commercial e-mail (UCE)] can be difficult if not impossible to identify without opening the message itself.

> *Having to take that extra step can be more than a waste of time and money*. Studies indicate that UCE often contains offensive subject matter, is a favored method for pursuing questionable if not fraudulent business schemes, *and has been successfully used to spread harmful computer viruses*. (emphasis added.)

(1st Dist. 2002) 94 Cal. App. 4th 1255, 1268.

The California Legislature recognized the threat of computer viruses from spam when it enacted Section 17529:

> (i) Many spammers have become so adept at masking their tracks that they are rarely found, and are so technologically sophisticated that they can adjust their systems to counter special filters and other barriers against spam and can even electronically commandeer unprotected computers, turning them into spam-launching weapons of mass production.

Bus. & Prof. Code § 17529(i). Therefore, one of the purposes of Section 17529.5 is to protect consumers from opening deceptive spam and to protect them from *other* recipients who opened spam and had their computers hijacked into sending even more spam.

Opening or viewing an unfamiliar email can expose a recipient's computer to computer viruses, malware or Trojan horses. The United States Computer Emergency Response Team has noted that:

> Most viruses, Trojan horses, and worms are activated when you open an attachment or click a link contained in an email message. If your email client allows scripting, then *it is possible to get a virus by simply opening a message*. It's best to limit what HTML is available in your email messages. The safest way to view email messages is in plain text.

https://www.us-cert.gov/publications/virus-basics (last viewed on August 9, 2014) (emphasis added). *See also ZooBuh, Inc. v. Better Broadcasting, LLC*:

> Industry also warns of rendering HTML in email messages …These e-mails can expose the unwary user to hostile viruses or other intrusive programs . . . The common theme here is

> end-user security. Malicious e-mailers can bury a wide variety of harmful actions within the HTML e-mail, including programs that activate upon download.

No. 2:11-cv-00516-DN *22-24 (D. Utah May 31, 2013) (Memorandum Decision and Order Granting Default Judgment).

Opening spam can activate "web bugs" (also known as "web beacons") embedded in the email. A web bug is an invisible graphic in an email message (or on a web page) that monitors, records, and alerts a third party as to who is reading the email message. Web bugs are often invisible because they are typically only 1-by-1 pixel in size with no border and colored the same as the background. *See* "The Web Bug FAQ," *available at* https://w2.eff.org/Privacy/Marketing/web_bug.html (last visited April 7, 2015). Web bugs provide spammers with information about who is opening their spams:

> 11. Why are Web Bugs used in "junk" Email messages?
>
> To measure how many people have viewed the same Email message in a marketing campaign.
>
> To detect if someone is viewed a junk Email message or not. People who do not view a message are removed from the list for future mailings.

Id. *See also* National Cyber Alert System, Cyber Security Tip ST04-007, *available at* https://www.us-cert.gov/ncas/tips/ST04-007 (last visited April 7, 2015) stating: "Many spammers send HTML mail with a linked graphic file that is then used to track who opens the mail message – when your mail client downloads the graphic from their web server, they know you've opened the message."

Therefore, if *Rosolowski* stands, spammers will continue to use deceptive header information such as false or generic From Display-Names to trick and entice California residents into opening their emails, exposing them to even more spam and possibly computer viruses, malware, and

Trojan horses. This is one of the very harms Section 17529.5 is supposed to prevent.

C. In Drafting Section 17529.5, The Legislature Made a Knowing Distinction Between Header and Content of an Email and Therefore Did Not Intend for Deception Within a Header to Be Corrected by the Body.

The plain language of Section 17529.5 shows that the legislature intended for deception contained within the From field to be actionable, without regard to the content of the email.

Two subsections of 17529.5 identified and differentiated the header and content of an email. In Section 17529.5(a)(2) the legislature prohibited deceptive headers, and in the very next subsection 17529.5(a)(3) the legislature prohibited subject lines that may mislead a recipient about the contents of the message.

If the legislature had intended for the contents of the email to correct the deception contained within the header, the legislature would have made that intention known when the legislature drafted and passed SB1457 in 2004. When it amended the section, the legislature was aware that the CAN-SPAM Act required the advertiser to identify itself in the email. 15 U.S.C. § 7704(a)(5)(iii). SB1457 was specifically written as a response to the passage of the CAN-SPAM Act[11]. Despite the CAN-SPAM Act requiring that the advertiser be identified in the email body, the California legislature made no reference to email content in Section 17529.5(a)(2), but did in Section 17529.5(a)(3).

[11] *See* Bill Analysis for SB 1457, Legis. Analyst, analysis of Sen. Bill No. 1457 (2003-2004 Reg. Sess.) p.1, available at http://leginfo.ca.gov/pub/03-04/bill/sen/sb_1451-1500/sb_1457_cfa_20040613_185546_asm_comm.html.

III.
MATERIAL MISREPRESENTATIONS AND DECEPTION UNDER CAN-SPAM ARE MATERIALLY DECEPTIVE FOR PURPOSES OF SECTION 17529.5

A. CAN-SPAM Sets a National Standard For Materially False or Misleading Header Information

CAN-SPAM sets the national standard of what constitutes "materially false or materially misleading header information." As the Ninth Circuit held in *Gordon v. Virtumundo* (9th Cir. 2009) 575 F. 3d 1040, 1062-63:

> [T]he CAN-SPAM Act prohibits only deceptive subject line headings or materially false or materially misleading header information. See 15 U.S.C. § 7704(a); accord 15 U.S.C. § 7701(b)(2) ("[S]enders of commercial electronic mail should not *mislead* recipients as to the source or content of such mail." (emphasis added)). Significantly, Congress intended this standard to regulate commercial e-mail messaging practices "on a nationwide basis."[21] 15 U.S.C. § 7701(b)(1). It was because the patchwork of state laws had proven ineffective that Congress sought to implement "one national standard," S.Rep. No. 108-102, at 21, applicable across jurisdictions.

California courts have also noted that CAN-SPAM sets a national standard for commercial email. In *Hypertouch, Inc. v. ValueClick, Inc.* (2011) 192 Cal. App. 4th 805, 829 the court held:

> We agree that the CAN-SPAM Act was intended to establish uniform standards for the content of commercial e-mail. The substantive provisions of the Act make clear that this "uniform standard" includes prohibitions on the use of "materially false or materially misleading header information," as well as deceptive subject lines that are likely to mislead the recipient of a commercial e-mail.

Therefore, if header information is materially false or misleading under CAN-SPAM, it is also materially false and misleading under Section 17529.5(a)(2) because CAN-SPAM sets the national standard.

B. CAN-SPAM Defines Materially Deceptive Headers

The CAN SPAM Act defines materially deceptive header information as:

> For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would *impair the ability of a recipient* of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency *to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.*

18 U.S.C. § 1037(d)(2) (emphasis added.)

The CAN-SPAM Act also proscribes in pertinent part:

> Whoever, in or affecting interstate or foreign commerce, knowingly—
>
> (3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,
>
> (4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names [ ].

18 U.S.C § 1037(a).

Furthermore, CAN-SPAM also further defines materially misleading headers as:

> header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading;

15 U.S.C. § 7704(a)(1)(A).

The Federal Trade Commission is the federal agency charged with enforcing the CAN-SPAM Act. 15 U.S.C. § 7702(3); 15 U.S.C. § 7706(a). Courts should grant considerable weight, if not deference, to its interpretations of CAN-SPAM. *Chevron USA Inc. v. Natural Resources Defense Council, Inc*. (1984) 467 US 837, 844-845. The FTC identified the From Display-Name as the first item in misleading header information in its guide to CAN-SPAM compliance when it stated:

> 1. Don't use false or misleading header information. Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.

CAN-SPAM Act: A Compliance Guide for Business available at: http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business (September 2009).

California courts have applied the CAN-SPAM definition of routing headers to Section 17529.5(a)(2). *Kleffman v. Vonage Holdings Corp*, (2010) 49 Cal. 4th 334, 340 n.5,[12] and *Balsam v. Trancos, Inc*. (2012) 203 Cal. App. 4th 1083, 1092, 1097. The CAN-SPAM definitions of materially misleading headers should also apply under Section 17529.5(a)(2) because CAN-SPAM sets a national standard and Section 17529.5 should be construed as broadly as possible to affect its stated statutory purpose: to prevent spam under the falsity or deception exception to the preemption provision of the CAN-SPAM Act.

Courts that have previously interpreted the scope of Section 17529.5 have missed two things. First, CAN-SPAM makes it illegal to *impair* the

[12] *But see* n. 6 *supra*: *Kleffman* notes that the California Legislature *rejected* the federal definition of email headers that only referred to routing information. CAN-SPAM apparently failed to consider that subject lines are also part of email headers.

ability to identify the sender of the email - not impossible," but simply more difficult. *U.S. v. Kilbride* (9th Cir. 2009) 584 F. 3d 1240, 1258. Second, using domain names "obtained by means of false or fraudulent pretenses or representations" may also make email headers materially misleading regardless of whether the information was technically truthful. 15 U.S.C. § 7704(a)(1)(A).

Under CAN-SPAM, materially misleading header information is that which impairs the ability to identify the sender, but CAN-SPAM does not set the criteria at "impossible."

C. Under CAN-SPAM, The Body of an Email Cannot "Cure" Materially False or Misleading Header Information

Under CAN-SPAM, the text or body of an email cannot cure misrepresentations in the header information. In *Facebook v. Power Ventures, Inc.* (ND CA February 16, 2012) No. C 08-05780 JW *12-14 (Order Granting Plaintiff's Summary Judgment and Denying Defendant's Summary Judgment), the court held:

> Defendants contend that even if the Court finds that they did initiate the e-mails at issue, they cannot be held liable for violations of the CAN-SPAM Act on the grounds that: (1) the text of the emails itself includes information about Power.com; and (2) Defendants had no control over the headers of the e-mails. The Court finds that both of these contentions are unavailing. First, the presence of a misleading header in an e-mail is, in and of itself, a violation of the CAN-SPAM Act, insofar as the Act prohibits the use of misleading header information. Thus, the fact that the text of the e-mails at issue may have included information about Power.com is irrelevant, for purposes of liability under the Act.

Under CAN-SPAM, the body of an email cannot cure the material misrepresentations in the header information and, because CAN-SPAM sets the national standard, the body of an email cannot cure header violations of Section 17529.5(a)(2) either.

D. Using Proxy Registered Domain Names to Send Spam May Violate CAN-SPAM Regardless of the From Name

One federal district court has interpreted 15 U.S.C. § 7704(a)(1)(A)'s language of "obtained by means of false or fraudulent pretenses or representations" to mean that falsified domain registration information can violate Section 17529.5. *ZooBuh, Inc. v. Better Broadcasting, LLC* (D. Utah May 31, 2013) No. 2:11-cv-00516-DN *18 (Memorandum Decision and Order Granting Default Judgment) defined it and held:

> Header Violations under the CAN-SPAM Act are not limited to false or misleading header information. Under 15 U.S.C. § 7704(a)(1)(A), even header information that is technically accurate violates the CAN-SPAM Act when the email "includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations." 15 U.S.C. § 7704(a)(1)(A).
>
> When a party registers a domain name with an ICANN compliant domain registrar, that registrant enters into a registration agreement with the domain registrar. In most, but not all cases, the domain registration agreement and the accompanying Terms and Conditions (collectively "Registration Documents") prohibit the use of the registered domain to send unsolicited commercial email or engage in other SPAM practices. Accordingly, in order to obtain the domains from the registrar, the registrant represents that it does not intend to use, and will not use, the domains for any purpose prohibited by the Registration Documents. If, as is the case here, the registrant does intend to use the domains for prohibited purposes, the registrant obtained the domains under a false pretense, and the sending of any email in violation of the Registration Documents violates 15 U.S.C. § 7704(a)(1)(A) on a per email basis.

In *Zoobuh*, the district court noted that the registrars eNom, Inc. and Moniker Online Services, LLC both required the party registering the

domain to accept its Registration Documents. The Registration Documents contained provisions whereby the registrant indicates that it will not use the domain name for purposes of sending unlawful commercial email or spam. *Id*.

Registrars also require registrants' truthful information to be disclosed in the Whois Database. Therefore, willfully providing false or incomplete information in the registration means that the registrant obtained the domain name by fraud.

While registrars and proxy-registration services are not synonymous,[13] many proxy-registration services also have terms and conditions prohibiting users of their services from sending spam.[14] Here, if any of the sending domains were proxy-registered to services that prohibited the sending of spam, or registered using false WHOIS information, then the header information of those emails would be materially misleading under 15 U.S.C. § 7704(a)(1)(A) *regardless* of the From Display-Name and would violate Section 17529.5(a)(2). Additionally, if any of the emails were sent from domains that were registered through a registrar that prohibits people from using the domains for spam, then those emails would also violate both 15 U.S.C.

---

[13] A registrar enables a registrant to create a domain name. A proxy-registration service takes legal ownership of a domain name and becomes the registered name holder, while licensing use back to the creator. The practical effect is that the proxy-service's information appears in the Whois database, thereby hiding the identity of the person who created the domain name. Proxy-registering domain names is a common spammer ploy to avoid detection.

[14] *See e.g.* Whois Guard Terms of Service ¶4(g) at http://www.whoisguard.com/legal-tos.asp; and Domains by Proxy Domain Name Proxy Agreement, Representations and Warranties at https://www.domainsbyproxy.com/policy/ShowDoc.aspx?pageid=domain_nameproxy.

§ 7704(a)(1)(A) and Section 17529.5(a)(2). However, the Appellant here did not provide any evidence to support either possible theory of liability in his summary judgment opposition. Therefore, the summary judgment below should be affirmed with clarification of the state of the law.

IV.
COURTS SHOULD CONSTRUE SECTION 17529.5 BROADLY, CONSISTENT WITH ITS PURPOSE: TO PREVENT DECEPTIVE SPAM

Section 17529.5 is a subsection of Business & Professions Code Section 17529 *et seq*. The purpose of Section 17529 is set forth in Section 17529(m):

> Because of the above problems, it is necessary that *spam be prohibited and that commercial advertising e-mails be regulated* as set forth in this article. (emphasis added).

Section 17529.2 sets forth in pertinent part:

> Notwithstanding any other provision of law, a person or entity may not do any of the following:
>
> (a) Initiate or advertise in an unsolicited commercial e-mail advertisement from California or advertise in an unsolicited commercial e-mail advertisement sent from California.
>
> (b) Initiate or advertise in an unsolicited commercial e-mail advertisement to a California electronic mail address, or advertise in an unsolicited commercial e-mail advertisement sent to a California electronic mail address.

Courts should construe statutes consistent with legislative intent. *Smith v. Superior Court* (2006) 39 Cal.4th 77, 83 states:

> In construing a statute, our fundamental task is to ascertain the Legislature's intent so as to effectuate the purpose of the statute. We begin with the language of the statute, giving the words their usual and ordinary meaning. The language must be construed in the context of the statute as a whole and the overall statutory scheme, and we give significance to every word, phrase, sentence, and part of an act in pursuance of the

> legislative purpose. In other words, we do not construe statutes in isolation, but rather read every statute with reference to the entire scheme of law of which it is part so that the whole may be harmonized and retain effectiveness. If the statutory terms are ambiguous, we may examine extrinsic sources, including the ostensible objects to be achieved and the legislative history. In such circumstances, we choose the construction that comports most closely with the Legislature's apparent intent, endeavoring to promote rather than defeat the statute's general purpose, and avoiding a construction that would lead to absurd consequences. [internal citations and quotations omitted.]

But for the passage of the federal CAN-SPAM Act, *all* spam would be illegal in California. Cal. Bus. & Prof. Code § 17529.2. The federal CAN-SPAM Act does not preempt state laws to the extent they proscribe falsity or deception. 15 U.S.C. § 7707(b)(1). To the extent that the CAN-SPAM Act itself defines header information as materially misleading or deceptive, by definition it would not preempt California law that imposes liability for the same misleading or deceptive header information. Thus, header information that violates CAN-SPAM constitutes a material violation of Section 17529.5.

V.
CONCLUSION

This Court should affirm the holding of the lower court because the Respondents met their burden of production on summary judgment that their emails did not violate California Business and Professions Code Section 17529.5(a)(2) and the Appellant failed to produce evidence to create a triable issue of material fact.

However, this Court should also find that From Display-Names that do not truthfully identify the sender or the advertiser violate Section

17529.5(a)(2), because the From Display-Name is one of the few pieces of header information that an email recipient sees before opening the email.

Furthermore, this Court should provide lower courts with the proper guidance when interpreting California Business and Professions Code Section 17529.5 in general by noting that the law should be interpreted expansively.

Emails that violate CAN-SPAM also violate Section 17529.5.

Dated: April 8, 2015

WALTON TWU LLP
/s/ Timothy Walton
Timothy Walton
Attorneys for *Amicus Curiae* CAUCE *et al*

CERTIFICATE OF WORD COUNT

(California Rules of Court, Rule 8.204(c)(1)

The text of this brief consists of 4,936 words, excluding tables and this certificate, as counted by the Microsoft Word 2013 word processing program used to generate the brief.

Dated: April 8, 2015

WALTON TWU LLP
/s/ Timothy Walton
Timothy Walton
Attorneys for Amicus Curiae CAUCE *et al*