

Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 28 • NUMBER 10 • OCTOBER 2016

Winning the Fight Against Email Spam Plaintiffs

By Karl Kronenberger

There have been many changes in the realm of email spam law since 2003, which was the year when both the federal CAN-SPAM Act and the California anti-spam law were passed. While the pendulum has swung in the slight favor of spam defendants in the past year, there have been multiple shifts in the laws since 2003.

Background

In the eight or so years after these spam laws were passed, most significant litigation was in federal court under the CAN-SPAM Act. This law provides standing only to web service providers (ISP) and government enforcers, so there were many early fights over whether a plaintiff truly was an ISP, and whether the ISP plaintiffs were truly damaged by experiencing any “adverse effects” as a result of emails received. As federal courts became more restrictive in their interpretation of standing under the federal law, many spam plaintiffs started to bring lawsuits under the California state law instead. While such lawsuits have existed since the enactment of the California statute, the recent trend is for attorneys to aggregate many plaintiffs in order to amass enough emails for six figure, and even seven figure, demands. This trend has grown as

a result of the liberal standing requirements under the California statute, as well as some cases that found that advertisers were strictly liable for the acts of their independent email publishers.

California’s Anti-Spam Law

The California anti-spam law¹ (the CASL) generally allows individuals (not just ISPs) to sue for statutory damages of up to \$1,000 per email. The CASL contains three categories of unlawful spam email that give rise to liability for both advertisers and senders of commercial emails:

- *A1 Violations*: The use of a sending domain name without the permission of the owner of that domain name;²
- *A2 Violations*: The use of false, forged or misrepresented header information, which includes the From email address, From name (*aka* Friendly From), and IP address of sending mail server;³ and
- *A3 Violations*: The use of a misleading subject line.⁴

Balsam v. Trancos, Inc.

Since 2014, the law has been changing to the benefit of spam defendants. This change, though, should be viewed in the context of a 2012 case, *Balsam v. Trancos, Inc.*⁵ In that case, Dan Balsam, the plaintiff and a California attorney, argued that seven

Karl Kronenberger, a partner at Kronenberger Rosenfeld, LLP, in San Francisco, represents advertisers, ad networks, and affiliate publishers in spam lawsuits and in spam law compliance matters. He can be reached at karl@krinternetlaw.com.

emails that he received from the defendant constituted A2 violations because defendant went to great lengths to hide its identity, and the identities of the sender and advertiser. Balsam argued that there was no way to trace the seven emails back to any person or business based on the contents of the emails themselves, or by viewing the public WHOIS record for the domain names used to send the emails.⁶ The court held that six of the emails were indeed violations of the CASL, and established a “tracing” methodology to determine whether email header information was falsified, misrepresented, or forged under A2. The court held that the inability to trace an email back to its sender using a publicly-accessible database, such as WHOIS, constituted an A2 violation under the CASL.

Post-Trancos Rulings

After the *Trancos* ruling in 2012, spam plaintiffs argued that emails violated the CASL if one could not trace emails to the senders, using information in the email headers and in the publicly available WHOIS database. Spam plaintiffs made this argument, regardless of what was contained within the body of the email, even if the body of the email contained the name and address of the sender. Notably, in 2010, the California Supreme Court, in the case of *Kleffman v. Vonage Holdings Corp.*,⁷ had ruled that the use of random or garbled domain names as sending domain names in commercial email does not violate the CASL. Thus, the argument that the body of an email should not be considered in assessing legal compliance was highly frustrating to email marketers who disclosed their identities in the bodies of emails but used untraceable domain names for sending emails.

Spam plaintiffs across California suffered a significant setback in 2014 with the decision in *Rosolowski v. Guthy-Renker, LLC*.⁸ In *Guthy*, the court reigned in the expansive arguments spam plaintiffs were making under *Trancos* and provided a road map for a more common sense approach to analyzing whether commercial email violates the CASL. The emails in *Guthy* had From lines that were not corporate names or registered fictitious company names, but, instead, the From lines contained the brand names of the marketed products (e.g., “Wen Hair Care,” “Proactiv Special Offer”). The plaintiff argued that the use of brand names

in the From line was misleading and an A2 violation because one could not identify the sender from merely the brand. The plaintiff also alleged that the words, “free gift,” in the subject line were misleading and an A3 violation because there were contingencies for the gift in the email body (i.e., one had to order a product to get a free gift). The court found, however, that because the identity of the sender was ascertainable through the body of the email, and because the body of the email clearly set forth the contingencies required to obtain the “free” gift, there was no material misrepresentation and, therefore, no violation of either A2 or A3 of the CASL.

Post-Guthy Decisions

Guthy was a significant departure from the *Trancos* case because *Guthy* took into account the information contained within the body of the email, and opened matters up to a more common sense analysis. Subsequent unpublished decisions have followed the reasoning of *Guthy*, finding that, if the body of an email provides the identity of the sender and clarifies any representations made in the subject line, then there is no A2 or A3 violation of the CASL.

For example, in *DeWitt v. DeVry Univ., Inc.*,⁹ the plaintiff, a California attorney, argued that multiple defendants violated A2 of the CASL because the sending domain names were not traceable to the sender, despite the fact that the brands advertised were in the From names and the advertisers were disclosed prominently in the body of the emails. The appellate court clearly stated, “He is wrong.”¹⁰ The court clarified that email header information violates A2 of the CASL if it neither identifies the sender in the body nor is traceable using a public WHOIS database.¹¹

In another case brought by Mr. Dewitt, *DeWitt v. Foot Locker Retail, Inc.*,¹² the court clarified that when the sending domain itself identifies the sender, there can be no A2 violation under the CASL. Thus, even if the sender is not traceable using the WHOIS record, other information in the email may be used to identify the sender, such as the sending domain name itself.¹³

Regarding subject lines, *Guthy* does not give marketers an absolute right to use the word, “free,” in subject lines, and several later cases have found violations based on material misrepresentations in subject lines. For example, in *Wagner v. Spire Vision*,

LLC, et al.,¹⁴ an email promised its recipient \$25 in return for completing a survey. The body of the email contained hyperlinks to web pages containing contingencies, but there was no mention of additional contingencies in the body of the email. The court denied the defendants' request for summary judgment, finding that these subject lines may be materially misleading and may constitute A3 violations under the CASL.

A1 Violations

While there is plenty of CASL case law providing examples of what constitutes A2 violations (deceptive headers) and A3 violations (deceptive subject lines), there is little to no guidance for marketers on what constitutes an A1 violation (use of domain without permission of owner). Section A1 of the CASL prohibits emails that contain or are accompanied "by a third-party's domain name without the permission of the third party." Because "permission" tends to be a fairly black or white issue, alleged A1 violations are easier arguments for spam plaintiffs to make. In fact, some spam plaintiffs see A1 violations as "slam dunks" and demand much more money to settle compared to A2 and A3 violations. If a commercial email uses a major brand without permission (e.g., Disney.com or Coca-cola.com), there is not much of an argument to be made in defense. Spam plaintiffs also have argued that the use of free email accounts to send email (such as Gmail.com or Yahoo.com) is a violation, because the terms of service for these free email services prohibit the sending of bulk email.

One argument that courts have not addressed is whether the use of a domain name without the permission of the owner is material enough of a violation to overcome preemption by the CAN-SPAM Act.

One argument that courts have not addressed is whether the use of a domain name without the permission of the owner is material enough of a violation to overcome preemption by the CAN-SPAM Act, which does not have a provision similar to A1 of the CASL. Many if not most email recipients only see the "friendly From" name and not the

actual sending email, so for these recipients there is no way for them to be misled. Further, many state and federal courts have held that non-material misrepresentations may not be violations of state spam laws because the carve out in CAN-SPAM that permits state spam laws to exist only carves out state spam laws the prohibit material misrepresentations.¹⁵ Unfortunately, until a court rules on this preemption argument, it likely will fall on the deaf ears of spam plaintiffs.

Popular New Tactics

In addition to focusing on A1 violations, there are other tactics that have become popular recently with spam plaintiffs. For instance, spam plaintiffs use automated systems to log in to their clients' email accounts and view, sort, assess, and download bulk commercial email solely for the purpose of initiating spam lawsuits. In fact, spam plaintiffs frequently never view the spam before filing suit, but instead the spam is gathered and viewed only by attorneys using automated systems.

One consequence of the use of automated systems, intended or not, is that the automated systems trigger views of the emails they gather, which in turn cause the mailing programs of marketers to send more email to that recipient, thus increasing potential damages by \$1,000 for each additional email sent. This practice obviously creates a defense for email marketers, as spam plaintiffs cannot request to be harmed and then sue for redress of such harm. There is a general maxim of tort law dating back ages that provides that, "[o]ne who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it."¹⁶ This maxim is reflected in the principle known as, *volenti non fit injuria* (literally, "to a willing person it is not a wrong"). California has even codified this principle in its statutes: "He who consents to an act is not wronged by it."¹⁷

Spam plaintiffs also are aggregating plaintiffs in order to increase potential settlements. When the use of automated systems, causing more email to be sent, is combined with the tactic of aggregating 10 or more plaintiffs, the total demand may be in the low to mid-six figures. Thus settlement demands in current spam lawsuits under the CASL are much different from the \$2,000 to \$5,000 demands that were common a decade ago.

Even with six figure demands from spam plaintiffs, though, current settlements (and judgments, for that matter) are not exceeding the litigation costs of defending the case. In other words, defendants will spend less, and often significantly less, if they settle a spam case compared to conducting discovery, trying the case to a jury, and hopefully prevailing. And in settlement negotiations, spam plaintiffs are keenly aware of defendants' litigation costs.

How to Reduce the Risk of Spam Liability

What should marketers do to reduce the risk of spam liability? The following are some suggestions.

1. *Avoid A1 Violations.* First, develop a compliance program to ensure that email publishers are using domain names that they own or have permission to use. Avoiding A1 violations (use of domains without permission) is perhaps the easiest way to reduce spam litigation risks today.
2. *Brands in Friendly From Names.* Despite the *Guthy* ruling that allows an analysis of the body of the email in assessing whether there is an A2 (deceptive header) violation, it is still best to use the brand name of the product advertised as the friendly From, or even better to use a company name or registered fictitious business name.
3. *List Contingencies in Email Body.* For promotional language such as "free" in subject lines, or any other assertion about offer terms, always insert all contingencies in the body of the email. Bear in mind that spam plaintiffs are creative, and they will look for subject line language that is arguably an offer term, with contingencies not detailed in the email body.
4. *Open WHOIS Records.* *Guthy* eviscerated the *Trancos* argument that all sending domains must be traceable to the sender using the WHOIS record without looking at the email body. However, it is best to eliminate all arguments of spam plaintiffs that the sender is not adequately identified in the body of the email. Thus it is best for email senders not to use privacy services to hide WHOIS domain ownership information.

5. *Comply with CAN-SPAM.* While this article did not provide a survey of all the technical requirements of the federal CAN-SPAM Act (name and address of sender, disclosure of commercial nature of email, opt-out link, honoring opt-outs, etc.), any email compliance program should ensure that senders are complying with these basic, and easy to implement, requirements.

While these guidelines will reduce the risk of spam litigation, the *Guthy* and *Trancos* decisions illustrate how the spam law landscape changes frequently. So, in addition to reducing risk with a compliance program that integrates the above guidelines, marketers need to be aware of new case law and changes in spam plaintiffs' tactics.

Notes

1. Bus. & Prof. C. 17529.5.
2. Bus. & Prof. C. 17529.5(a)(1).
3. Bus. & Prof. C. 17529.5(a)(2).
4. Bus. & Prof. C. 17529.5(a)(3).
5. *Balsam v. Trancos, Inc.*, 203 Cal. App. 4th 1083 (2012).
6. A WHOIS database record displays the registered owner of a domain name.
7. *Kleffman v. Vonage Holdings Corp.*, 232 P.3d 625 (2010).
8. *Rosolowski v. Guthy-Renker, LLC*, 230 Cal. App. 4th 1403 (2014).
9. *DeWitt v. DeVry Univ., Inc.*, No. A142444, 2015 WL 4120482, at *1 (Cal. Ct. App. July 8, 2015), *review denied* (Sept. 30, 2015).
10. *Id.* at 9.
11. *Id.*
12. *DeWitt v. Foot Locker Retail, Inc.*, No. A141847, 2015 WL 3417439, at *4 (Cal. Ct. App. May 28, 2015).
13. *See, id.* at 4 ("Here, the sender domain name, [Footlocker@e.footlocker.com], 'identifies the actual sender on its face'—Foot Locker.").
14. *Wagner v. Spire Vision, LLC, et al.*, 2015 WL 876514 (N.D. Cal. 2015).
15. *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348, 353 (4th Cir. 2006) ("Whatever the precise scope of the Oklahoma provision might be, we cannot agree that Mummagraphics' action for immaterial errors survives preemption.").
16. Restatement (Second) of Torts 892A (1979).
17. Cal. Civ. Code § 3515. *See also*, *Beyond Systems, Inc. v. Kraft Foods, Incorporated, et al.*, 777 F.3d 712, 718-19 (4th Cir. 2015) ("Beyond Systems' consent to—and indeed its solicitation of—the harm at issue in this case prohibits Beyond Systems from recovering under the Maryland and California anti-spam statutes.").

Copyright © 2016 CCH Incorporated. All Rights Reserved.
Reprinted from *Intellectual Property & Technology Law Journal*, October 2016, Volume 28, Number 10,
pages 11–14, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.wklawbusiness.com.

