

1 ("Biznesshosting"). According to the Government's allegations, within approximately two
2 hours after Biznesshosting provided Twombly with logon credentials, it began receiving
3 complaints regarding spam electronic mail messages originating from its network.
4 Defendants allegedly sent approximately 1 million spam electronic mail messages, followed
5 several days later by another 1.5 million. The spam messages allegedly contained
6 advertising for computer software, and directed recipients to the website of a software
7 company with an address in Canada. The Government alleges this website was falsely
8 registered under the name of a non-existent business, and that the messages' routing
9 information and "From" lines were falsified, preventing recipients, internet service providers,
10 and law enforcement agencies from identifying, locating, or responding to the senders.
11 Biznesshosting allegedly investigated the complaints, traced the spam to the server leased
12 by Defendant Twombly, and terminated his account.

13 The Government alleges the traffic generated by Defendant Twombly's leased server
14 led internet-based anti-spam services to blacklist Biznesshosting's network domain, resulting
15 in both immediate and continuing financial loss to Biznesshosting.

16 The Government alleges a search by the FBI uncovered approximately twenty
17 dedicated servers leased by Defendant Twombly using false credentials. Defendant
18 Twombly allegedly leased the servers for a man known only as "Josh," and was paid \$100
19 for each set of logon credentials he provided to "Josh." "Josh" was allegedly later
20 determined to be Defendant Eveloff. The Government alleges both Defendants caused the
21 spam messages to be sent.

22 **II. Legal Background**

23 The relevant sections of the statute under are as follows:

24 § 1037. Fraud and related activity in connection with electronic mail
25 (a) In general.--Whoever, in or affecting interstate or foreign commerce,
knowingly --

26 (3) materially falsifies header information in multiple commercial electronic
27 mail messages and intentionally initiates the transmission of such
messages, [or]

28 (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

1 transmission of multiple commercial electronic mail messages from any
2 combination of such accounts or domain names, . . .
shall be punished as provided in subsection (b).

3 Section 1037(d)(2) explains in part the meaning of § 1037(a)(3) and (4):

4 (2) Materially.--For purposes of paragraphs (3) and (4) of subsection (a),
5 header information or registration information is materially falsified if it is
6 altered or concealed in a manner that would impair the ability of a recipient
7 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.

8 III. Discussion

9 A. Motion to Dismiss for Vagueness

10 Overly vague penal statutes violate due process. The Supreme Court has explained:

11 Reviewing decisions in which we had held criminal statutes “void for
12 vagueness” under the Due Process Clause, we noted that this Court has
13 often recognized the basic principle that a criminal statute must give fair
14 warning of the conduct that it makes a crime. Deprivation of the right to fair
15 warning, we continued, can result both from vague statutory language and
16 from an unforeseeable and retroactive judicial expansion of statutory
language that appears narrow and precise on its face. For that reason, we
concluded that if a judicial construction of a criminal statute is unexpected
and indefensible by reference to the law which had been expressed prior to
the conduct in issue, the construction must not be given retroactive effect.

17 *Rogers v. Tennessee*, 532 U.S. 451, 457–58 (2001) (alterations, citations, and internal
18 quotation marks omitted). The standard, then, requires the statute’s language to give “fair
19 warning” and is violated by “unexpected and indefensible” judicial constructions of the
20 statute. *U.S. v. Howick*, 263 F.3d 1056, 1068 n.6 (9th Cir. 2001).

21 The standard is aimed at giving notice to a person of “ordinary intelligence” or
22 “common intelligence.” *Bouie v. City of Columbia*, 378 U.S. 347, 351 (1964). No more than
23 “fair warning” is required:

24 The root of the vagueness doctrine is a rough idea of fairness. It is not a
25 principle designed to convert into a constitutional dilemma the practical
26 difficulties in drawing criminal statutes both general enough to take into
account a variety of human conduct and sufficiently specific to provide fair
warning that certain kinds of conduct are prohibited.

27 *Colten v. Kentucky*, 407 U.S. 104, 110 (1972). A statute is merely required to give a person
28 of ordinary intelligence “a reasonable opportunity to know what is prohibited.” *Village of*

1 *Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498 (1982). The fair
2 notice requirement is determined by objective standards. *United States v. Kozminski*, 487
3 U.S. 931, 949–50 (1987).

4 The degree of vagueness that the Constitution tolerates depends in part on the nature
5 of the enactment. *Village of Hoffman*, 455 U.S. at 498. Economic regulation of businesses
6 is subject to less strict requirements, and a scienter requirement may mitigate a law’s
7 vagueness. *Id.* at 498–99. A statute that threatens to inhibit the exercise of constitutionally
8 protected rights may, however, require a stricter vagueness test. *Id.*

9 Defendants contend the meanings of “impair” and “materially” as explained in
10 § 1037(d)(2) are unconstitutionally vague. This section provides that

11 header information or registration information is materially falsified if it is
12 altered or concealed in a manner that would impair the ability of a recipient
13 of the message, an Internet access service processing the message on behalf
14 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.

15 Defendants argue that a header does not necessarily identify the sender, and that a
16 layperson has little or no ability to trace a sender’s location based on the address.

17 While it is true that email addresses do not necessarily on their face identify the
18 sender by name, this is beside the point. An email address may not identify who a sender
19 is, but it does tell a recipient where to send replies to the sender, much in the same way a
20 return address on an envelope identifies the sender of a letter and tells the recipient where
21 to send replies to. A material falsification of header or registration information can violate
22 this provision by hindering a recipient’s ability to respond to the sender of an email, which
23 is one of the provisions of § 1037(d)(2).

24 Defendants also argue that because laypeople’s ability to identify senders is
25 inherently impaired, the statute is meaningless. This is a straw man argument: the statute
26 at issue does not assume senders are personally identifiable from header information, nor
27 does it purport to require easy and perfect identification; it merely forbids fraudulent

28 ///

1 interference with users' ability to locate senders. The fact that individuals' ability to identify
2 senders is already limited does not necessarily mean that it cannot be impaired further.

3 Even if identifying senders by header information may be difficult for many laypeople,
4 Defendants have not shown it is equally difficult for all users. Nor is it impossible for anyone,
5 as Defendants imply. A layperson wishing to identify the sender of an email message may
6 be able to do so in several ways. For example, although Defendants claim no email hosting
7 service (e.g., Yahoo!, Hotmail, AOL, etc.) would ever identify the sender of an email if a
8 private person requested it, this is never substantiated. Moreover, there is no reason to
9 assume that an email hosting service would resist a subpoena or refuse to cooperate with
10 a government investigation. False header information would hinder either of these.

11 Furthermore, as the government points out, Defendants' argument is based solely on
12 the ability of an individual recipient to identify the sender of spam emails. These two
13 sections are expressly also designed to protect the ability of internet access services and
14 government agencies to investigate spam. Defendants fail to show that falsified header or
15 registration information would not impair the ability of either of these to investigate the source
16 of spam or identify senders.

17 This motion is therefore **DENIED**.

18 **B. Motion to Dismiss as Overbreadth**

19 The doctrine of overbreadth is primarily a First Amendment doctrine, although it also
20 covers a few other Constitutional protections not at issue here.² Unlike other facial
21 challenges, a challenge for overbreadth can succeed if a law punishes a substantial amount
22 of free speech "judged in relation to the statute's plainly legitimate sweep." *Virginia v. Hicks*,
23 539 U.S. 113, 118–19 (2003) (quoting *Broadrick v. Oklahoma*, 413 U.S. 601, 615 (1973)).

24
25 ² Although the Supreme Court recently suggested that overbreadth challenges can
26 be brought in a few other settings, see *Sabri v. United States*, 541 U.S. 600, 609–10, 124
27 S.Ct. 1941, 158 L.Ed.2d 891 (2004) (citing cases addressing the right to travel, the right to
28 abortion, and legislation under section 5 of the Fourteenth Amendment), the Court stated
that "[o]utside these limited settings, and absent a good reason, [it does] not extend an
invitation to bring overbreadth claims." *Id.* at 610, 124 S.Ct. 1941. Indeed, the Court
cautioned that "facial challenges are best when infrequent," and in particular, overbreadth
challenges "are especially to be discouraged." *Id.* at 609, 124 S.Ct. 1941.

1 The purpose of this doctrine is to permit a party to raise a challenge based on the potential
2 chilling effect of an overbroad statute on protected speech, even where protected speech
3 is not before the court. *Bates v. State Bar of Arizona*, 433 U.S. 350, 380 (1977). A
4 successful challenge under this doctrine invalidates all enforcement of the law unless and
5 until a limiting construction or partial invalidation so narrows it as to remove the apparent
6 threat or deterrence to constitutionally-protected expression. *Id.* at 119. Even if a criminal
7 statute is overbroad, a court may properly narrow it before considering if a conviction under
8 the narrowed statute would be proper. *Osborne v. Ohio*, 495 U.S. 103, 104 (1990).

9 In this case, however, the overbreadth doctrine does not apply. Sections 1037(a)(3)
10 and (4) specifically require as an element that the emails be “commercial.” “Commercial
11 electronic mail message” is defined in 15 U.S.C. § 7702. However, the overbreadth doctrine
12 does not apply to commercial speech. *Village of Hoffman*, 455 U.S. at 496–97 (citing *Central*
13 *Hudson Gas & Electric Corp. v. Public Service Comm’n*, 447 U.S. 557, 565 n.8 (1980)). This
14 is because “commercial speech is more hardy, less likely to be ‘chilled,’ and not in need of
15 surrogate litigators.” *Board of Trustees of State University of New York v. Fox*, 492 U.S. 469,
16 481 (1989). *But see S.O.C., Inc. v. County of Clark*, 152 F.3d 1136, 1143 (9th Cir. 1998)
17 (holding that statute reaching beyond purely commercial speech to chill fully protected
18 speech can merit application of the overbreadth doctrine). Because it is clear the challenged
19 portion of the statute governs only commercial speech, there is no reason to believe
20 protected, noncommercial speech would be chilled. The Court therefore finds no basis for
21 application of the overbreadth doctrine.

22 Even if the overbreadth doctrine were applicable, it would not help Defendants. Facial
23 overbreadth may not be invoked when “a limiting construction has been or could be placed
24 on the challenged statute.” *Broadrick*, 413 U.S. at 613; *accord Hicks*, 539 U.S. at 118–19.

25 This motion is therefore **DENIED**.

26 ///

27 ///

28 ///

1 **C. Motion for Dismissal for Failure to Allege *Mens Rea***

2 Defendants seek dismissal of the indictment because, they contend, it fails to allege
3 *mens rea*, an essential element. Defendants argue that although the statute includes the
4 *mens rea* “knowing,” implicit in the statute is the element of intent to commit a criminal act.
5 Defendants cite *U.S. v. Nguyen*, 73 F.3d 887 (9th Cir. 1995) in support of this. In that case,
6 the Ninth Circuit held that failure to advise jurors of the element of criminal intent — which
7 distinguished misdemeanor from felony alien smuggling — was prejudicial error. The Ninth
8 Circuit pointed out that the felony statute incorporated the *mens rea* of criminal intent, and
9 was not intended to penalize innocent conduct. In so doing, the Ninth Circuit made note of
10 the “*mens rea* requirement assumed to be an element of every common law offense.” *Id.*
11 at 893.

12 Defendants also cite *U.S. v. Du Bo*, 186 F.3d 1177, 1179–80 (9th Cir. 1999). There,
13 an indictment failed to allege knowledge or intent, the *mens rea* implicitly read into the Hobbs
14 Act. Therefore, the Court determined that the indictment, which merely alleged that the
15 defendant “unlawfully” affected commerce by “wrongful” use of force, was deficient. The
16 Ninth Circuit construes criminal statutes “in light of the fundamental principle that a person
17 is not criminally responsible unless ‘an evil-meaning mind’ accompanies ‘an evil-doing
18 hand.’” *U.S. v. Barajas-Montiel*, 185 F.3d 947, 952 (9th Cir. 1999) (citing *Morissette v.*
19 *United States*, 342 U.S. 246, 251 (1952)).

20 Section (a)(3) includes two *mens rea* elements: a defendant must “knowingly”
21 materially falsify header information, and then “intentionally” transmit it. Section (a)(4)
22 likewise includes two *mens rea* requirements: a defendant must “knowingly” register for
23 accounts using information that materially falsifies the registrant’s identity, and “intentionally”
24 send commercial emails from those accounts.

25 Depending on the context of the statute, different terms may be used to show criminal
26 intent. *Morissette*, 342 U.S. at 264 (“Congress . . . has seen fit to prescribe that an evil state
27 of mind, described variously in one or more such terms as ‘intentional,’ ‘wilful,’ ‘knowing,’
28 ‘fraudulent,’ or ‘malicious,’ will make criminal an otherwise indifferent act. . . .”) Here, section

1 (a)(3) requires a higher *mens rea* than general criminal intent; a defendant must “knowingly”
2 falsify header information and “intentionally” transmit it. Thus, a defendant must at the very
3 least know he is being deceptive while sending multiple commercial emails. Under
4 *Morissette*, and its progeny, this satisfies the “evil-meaning mind” requirement. See *U.S. v.*
5 *Yermian*, 468 U.S. 63, 74–75 (1984) (holding statute imposing criminal sanctions for
6 deliberately false statements submitted to federal agency, even without a showing that
7 defendant knew they were being submitted to the federal government, did not constitute a
8 “trap for the unwary”). Cf. *Liparota v. U.S.*, 471 U.S. 419, 432 n.15 (1985) (interpreting
9 *Yermian* as holding that requiring government to prove defendant knowingly and willingly
10 made a false statement satisfied the “evil-meaning mind” requirement with respect to that
11 element of the crime).

12 Although Defendants ask the Court to consider online deception an innocent
13 peccadillo or even a positive good,³ that is not the view of this statute, which is particularly
14 aimed at deception. Nor is it appropriate for reasons of policy. Deception, even where it is
15 not criminal, is neither innocent nor worthy of any constitutional protection — particularly in
16 the commercial context. See *BMW of North America, Inc. v. Gore*, 517 U.S. 559, 576 (1996)
17 (holding that trickery or deceit was one factor rendering a civil defendant’s conduct more
18 reprehensible, and supporting an award of punitive damages). See also *Bates v. State Bar*
19 *of Arizona*, 433 U.S. 350, 383 (1977) (“Advertising that is false, deceptive, or misleading of
20 course is subject to restraint.”); *Keeton v. Hustler Magazine, Inc.*, 465 U.S. 770, 776 (1984)
21 (“There is ‘no constitutional value in false statements of fact.’”) (quoting *Gertz v. Robert*
22 *Welch, Inc.*, 418 U.S. 323, 340 (1974)).

23 Section (a)(4) is open to two interpretations, depending on whether “knowingly”
24 modifies only “registers” or whether it also modifies “using information that materially falsifies
25 the registrant’s identity.” Although Defendants do not raise this, if the former interpretation

26
27 ³ Defendants raise this in the context of their overbreadth argument: “People have
28 been using false information to sign up for e-mail accounts since the internet went public. Anonymity was one of the great things about the internet. As written, section (a)(4) criminalizes a large category of innocent conduct.” (Motion filed November 1, 2006, at 3:24–26.)

1 is used, this section could potentially penalize innocent behavior, if an innocent agent were
2 to register and send emails. See *U.S. v. Alfonzo-Reyes*, 384 F. Supp.2d 523, 527 (D.P.R.
3 2005) (noting that routine ministerial task of submitting an application on behalf of another
4 person could not constitute a crime, where the person submitting the application did not
5 know it contained false information). The Court need not reach this hypothetical argument,
6 however. While the Court acknowledges some potential ambiguity in section (a)(4), it has
7 no application to the facts of this case.

8 The indictment largely tracks the language of the statute and thus refers to “knowing”
9 and “intentional” acts without mentioning general criminal intent. The indictment does not
10 end there, however. As part of Count 1 (section (a)(3)), the indictment specifically charges
11 that the two Defendants conspired to lease servers using false names. (Indictment at
12 2:23–24.) It alleges also that Defendant Twombly leased servers using false identities, or
13 fraudulently. *Id.* at 3–4 (alleging that Twombly “leased” or “fraudulently leased” dedicated
14 servers “using the false identity” or “under the false identity” of various fictitious people, or
15 “under a false name”). The indictment also alleges that Eveloff paid Twombly every time
16 Twombly leased a server using a false name. *Id.* at 4. The allegations therefore foreclose
17 the possibility of innocent behavior being penalized in this case.

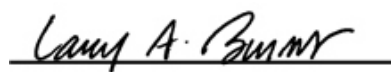
18 This motion is therefore **DENIED**.

19 **III. Conclusion and Order**

20 For these reasons, Defendants’ motions to dismiss the indictment are **DENIED**. The
21 Court has already accepted Defendant Twombly’s plea, and is informed Defendant Eveloff
22 is prepared to plead as well. All other pending motions are therefore **DENIED AS MOOT**.

23
24 **IT IS SO ORDERED.**

25 DATED: February 22, 2007

26 

27 **HONORABLE LARRY ALAN BURNS**
28 United States District Judge

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28