

1 Timothy J. Walton, Esq. (State Bar No. 184292)
WALTON & ROESS LLP
2 407 South California Avenue
Suite 8
3 Palo Alto, CA 94306
Phone (650) 566-8500
4 Fax: (650) 618-8687
Email: silverstein-experienced.internet@netatty.com

5
6 John L. Fallat, Esq. (State Bar No. 11482)
LAW OFFICES OF JOHN L. FALLAT
523 Fourth Street, Suite 210
7 San Rafael, CA 94901-3349
Phone: (415) 457-3773
8 Fax: (415) 457-2667

9 Attorneys for Plaintiff
HYPER TOUCH, INC.
10

11 **UNITED STATES DISTRICT COURT**

12 **NORTHERN DISTRICT OF CALIFORNIA (SAN FRANCISCO DIVISION)**

13	HYPERTOUCH, INC.,)	Case No.: C 04-5203 SI
)	
14	Plaintiff,)	DECLARATION OF WILLIAM K.
	vs.)	COLE IN SUPPORT OF
15)	PLAINTIFF'S OPPOSITION TO
	KENNEDY-WESTERN UNIVERSITY, et al.,)	MOTION FOR SUMMARY
16)	JUDGMENT
	Defendants.)	Date: February 10, 2006
17)	Time: 9:00 a.m.
)	Judge: Hon. Susan Illston
18)	
19)	

20 I, William K. Cole, declare:

21 1. I am over eighteen years of age and am a resident of Eastpointe, Michigan.
22

- 1 2. I have experience and expertise with the transmission of email messages because I have
2 been a professional systems administrator and computer networking consultant for 14
3 years. I am a recognized expert on the Stalker Internet Mail Server (SIMS) Software. I
4 have been involved in the direct operational prevention and tracking of spam since 1993.
- 5 3. After examining the Kennedy-Western University email and logs provided by
6 Hypertouch, Inc. and the analyses made by Lawrence Miller and Jason Rines, I have
7 reached the conclusions stated in this declaration.
- 8 4. I cannot find a single message in this entire collection that seems to me to be actually
9 compliant with the CAN-SPAM Act or California law. All of them include one or more
10 of: deceptive or blatantly forged headers; indication of the sender using a fraudulent
11 HELO argument for transport; likely unauthorized (and hence criminal) use of third-party
12 systems (commonly referred to as "zombies") for delivery; and use of deceptive HTML
13 coding, such as "title" attributes for anchor tags. All of those tactics serve no honest
14 purpose and serve to trick the reader of the message or the mail systems involved in
15 delivery about the nature and source of the messages and their links.
- 16 5. In one set of over 1000 messages sent during approximately one month and bearing
17 strong indications of 2 distinct senders, over 200 different apparent 'zombie' machines
18 were used to send Kennedy-Western's spam. It should be understood that even when
19 spam does not itself contain malicious software, it is the spam which is sent by those who
20 build and operate those networks of "zombie" machines which drives the continuing
21 flood of trojan-bearing email worms.

- 1 6. Most of the mail, from what appears to have been multiple senders, was sent through
2 machines which appear to have been compromised "zombie" machines, whose legitimate
3 owners very likely had no idea they were being used to send mail at all. This is a common
4 pattern in modern spam, most of which is sent through hijacked personal computers on
5 residential connections.
- 6 7. Evidence of fraud and deceptive practices are rampant among the emails I analyzed: false
7 HELO indications: no "verified" in the SIMS-generated Received headers, with log
8 entries that indicate SIMS got an actual negative response to attempted verification;
9 Blatantly false Received headers using a typical Sendmail structure right down to the
10 idiosyncratic Sendmail version markings, but with Queue ID fields that cannot be from
11 Sendmail; X-Mailer lines naming mailers that cannot construct HTML mail, on HTML
12 mail; Random data after HTML close tag, for which there is no point except as an
13 invisible "hashbuster" making the messages variant enough that some automated spam
14 detectors won't see them as the same; Misleading From headers; Faked Return-Path
15 headers that are not consistent with the envelope sender, which is what the Return-Path
16 header is supposed to contain when it is present; Postal addresses of unclear purpose, in
17 some cases in foreign countries, are included at the bottom of some messages. The only
18 point I can see for these is to mislead the recipient into thinking that some party other
19 than Kennedy-Western was responsible.
- 20 8. The bodies of the email indeed do point to KWU, and do include their address. Some of
21 these messages pull their image content and/or have links intended for the recipient to
22 click that refer directly to KWU systems (i.e. www.kw.edu) and others use content to

1 click targets from now-dead domains that appear to have belonged to professional
2 spamming operations. However, there are a number of common threads between many
3 different subsets of messages, and it seems far-fetched to suppose that these are not all in
4 fact sent on behalf of KWU and with their knowledge, since they share common text and
5 in many cases messages which seem otherwise unrelated have the same click targets
6 and/or use the same body images. The only alternative interpretation to these being all
7 sent on behalf of KWU is a massive campaign involving multiple criminal entities trying
8 to smear KWU, and that strains credibility.

9 9. My analysis of the data also puts into question some of the reasoning and hypothesis
10 presented in the report and declaration of Jason Rines that seems at odds with a
11 reasonable interpretation of the available data. The diversity of the email in specific
12 tactics of deception indicates to me that Kennedy-Western found multiple providers of
13 that service, and it is not plausible to me that Kennedy-Western was not actively seeking
14 precisely that sort of recipient deception service.

15 10. It is certainly possible for Kennedy-Western to have known the nature of the spam that
16 was being sent on their behalf. It is common practice in the bulk email business (as it is in
17 the postal direct advertising business) for a legitimate customer and legitimate
18 intermediaries and legitimate senders to all assure that they have special addresses on the
19 lists of those they pay to have email sent, to oversee the process and assure that the mail
20 is in fact being sent, that it has the right content, and that it is deliverable. For example, it
21 has long been a common practice for customers who really seek a legitimate "opt-in"
22 service to require that a service provider provide them with a means of testing exactly

1 how a user subscribes and what they see, and to use that to put secret test addresses on the
2 list. Because bulk email has been an industry dominated for all of its 10-year history by
3 scam artists specializing in deceiving both their customers and spam recipients, it has
4 been common and widely recommended for years for those seeking to buy emailing
5 services to fully verify that a service provider is in fact following whatever standards they
6 claim to follow. For Kennedy-Western to have not done so is not simply naive, it is
7 negligent.

8 11. The nature of the email in this litigation is a stark contrast with that of the legitimate bulk
9 email industry. Nothing I can find in these messages points at any legitimate bulk email
10 sender of any sort. Legitimate bulk mail senders do not forge headers. Legitimate bulk
11 mail senders maintain domains for long periods, because their domains are part of their
12 reputations. Legitimate bulk mail senders do not use false HELO arguments in SMTP.
13 Legitimate bulk mail senders do not use hashbusting tricks to evade filters. Legitimate
14 bulk mail senders do not use residential broadband services to send their mail.

15 12. As to the nature of Hypertouch, CAN-SPAM provides a clear definition of an ISP by
16 reference to 47 U.S.C. 231(e)(4). I would note that by KWU's definition and proposed
17 application of it, very few companies in existence would qualify because many ISP's
18 (including the largest ISP's in the USA other than Earthlink) are operated as secondary
19 businesses by companies whose largest and most profitable business is something else.
20 For example, AOL is a unit of TimeWarner, the new AT&T (formerly SBC) is a local and
21 long distance phone company, Comcast is a cable TV operator, etc.

1 13. As a small provider offering custom services for a small number of clients, Hypertouch is
2 perfectly normal in not having a published price list, as their services are not tarriffed and
3 the services they provide are different for each customer. In addition, the first section of
4 CAN-SPAM explaining the policy considerations behind it clearly refer to costs imposed
5 on businesses, and businesses who act as their own Internet access providers for the
6 purposes of email service actually make up the majority of email server operators on the
7 net. It seems perverse to me for standing to be restricted to public vendors of service
8 alone, instead of to providers of service, whether they sell mass-market services to
9 consumers, sell customized business services, or run their own services and provide them
10 only to their own employees.

11 14. The DNS and registrations for the domains involved and cited in the headers as part of
12 the Hypertouch mail system make it clear to anyone familiar with common practices of
13 mail service providers that Hypertouch is operating a mail system for multiple different
14 domains whose registrations indicate multiple different owners, a normal practice for any
15 such service provider.

16
17 I declare under penalty of perjury under the laws of the State of California and of the
18 United States that the foregoing is true and correct, and that this declaration was executed on
19 January 25, 2006, at Eastpointe, Michigan.

20 

21 _____
William K. Cole