

1 QUINN EMANUEL URQUHART OLIVER & HEDGES, LLP
2 Scott G. Lawson (Bar No. 174671)
3 scottlawson@quinnemanuel.com
4 Tyler G. Doyle (Bar No. 242477)
5 tydoyle@quinnemanuel.com
6 50 California Street, 22nd Floor
7 San Francisco, California 94111
8 Telephone: (415) 875-6600
9 Facsimile: (415) 875-6700

6 Attorneys for Plaintiff
Kimberlite Corporation

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA

11 Kimberlite Corporation, a California
12 Corporation

12 Plaintiff,

13 vs.

14 John Does 1-20

15 Defendants.

CASE NO. 3:08cv02147

**KIMBERLITE CORPORATION'S
OPPOSITION TO JOHN DOE'S
MOTION TO QUASH SUBPOENA
DIRECTED TO AT&T INTERNET
SERVICES**

19 **Preliminary Statement**

20 Defendant John Doe's threadbare Motion to Quash plaintiff Kimberlite
21 Corporation ("Kimberlite")'s subpoena to AT&T Internet Services offers no cogent
22 legal argument as to why the subpoena should be quashed and represents nothing
23 more than an attempt by Doe to delay discovery of information to which Kimberlite
24 is legally entitled.

25 As set forth in the complaint, on at least two occasions in April 2008, Doe,
26 using the IP address of 71.135.177.158, trespassed on Kimberlite's email system and
27 logged into the user accounts of several Kimberlite employees. While there, Doe
28 viewed email addressed to and intended for these employees, as well as confidential

1 and proprietary information belonging to Kimberlite, its employees, and its clients.
2 Doe did this without the authorization of Kimberlite or the individual employees
3 affected by the break-ins. Kimberlite has properly pleaded a violation of the
4 Computer Fraud and Abuse Act ("CFAA"), and a claim of trespass to chattels, and
5 has shown good cause for AT&T Internet Services, the owner of the IP address, (*see*
6 attached Exhibit B) to disclose his identity.

7 In moving to quash Kimberlite's valid subpoena, Doe argues that the Cable
8 Communication Policy Act of 1984 ("CCPA") prevents AT&T from disclosing his
9 identity, and that the Computer Fraud and Abuse Act ("CFAA") does not apply to
10 his conduct. Neither argument is a legitimate basis for quashing a subpoena.

11 The law is clear, moreover, that the CCPA is wholly inapplicable here, as this
12 Act regulates dissemination of subscriber data by operators of cable systems, and
13 not telecommunications companies such as AT&T. Kimberlite has, furthermore,
14 satisfied all elements for establishing a violation of the CFAA. To succeed on a
15 CFAA claim, Kimberlite need only show that Doe knowingly accessed a protected
16 computer, that Doe did so without authorization or exceeded authorized access, that
17 the computer broken into was involved in interstate commerce, and that the
18 Company suffered at least \$5,000.00 in damages in the past year as a result of Doe's
19 actions. Kimberlite has properly pleaded all these elements, and has documented at
20 least some of the break-ins and damages caused by Doe's conduct.

21 John Doe has presented no colorable argument as to why Kimberlite's
22 subpoena to AT&T Internet Services should be quashed. His motion should be
23 denied.

24 **Summary of Facts**

25 Kimberlite Corporation is the world's largest independent dealer of Sonitrol
26 brand security systems. Kimberlite both installs and monitors security systems for
27 its customers, and as a result, customers provide the company with a great deal of
28 confidential and proprietary information via email. Moreover, Kimberlite also

1 regularly discusses its own confidential and proprietary information on its email
2 system.

3 In April 2008, Kimberlite Corporation discovered two unauthorized breaches
4 of its internal computer network. (See Kimberlite Complaint at ¶¶ 8-9; Deedon
5 Decl. at 1; Exhibit C). The breaches took place on April 7, 2008 and April 14, 2008,
6 and both originated from the IP address 71.135.177.158. (*Id.*) In both cases, John
7 Doe accessed Kimberlite email accounts assigned to various employees and then
8 proceeded to view the content of email messages not intended for him. At no time
9 did Doe have the authorization of either Kimberlite or the affected employees to
10 view these email messages. (*Id.*)

11 Upon discovering the initial breaches, Kimberlite brought the instant action
12 and undertook an investigation of the illegal intrusions into its internal computer
13 network. (Deedon Decl. at 1.) This investigation involved the Company's IT
14 Department, outside counsel, and private investigators. (Patterson Decl. at 1.) The
15 Company's investigation revealed that in the period April 2-15, 2008, John Doe used
16 the same AT&T IP address to commit 26 additional unauthorized breaches of the
17 Kimberlite email system. (See Deedon Decl. at 1; Exhibit D.) A subpoena was
18 served on AT&T Internet Services on April 28, 2008 (Exhibit A) to ascertain the
19 identity of the user of IP address 71.135.177.158 at the times at which two of these
20 email break-ins took place. On May 7, 2008, John Doe then filed a Motion to
21 Quash the subpoena.

22 Argument

23 **I. KIMBERLITE SERVED A VALID SUBPOENA UPON AT&T**

24 The Federal Rules of Civil Procedure obligate third parties to produce
25 documents or information responsive to a subpoena that a party serves on them.
26 Fed. R. Civ. P. 45(b), (d). If the information is relevant and there is good cause for
27 their production, the subpoena is enforced unless the documents are privileged or
28

1 the subpoena is unreasonable, oppressive, annoying, or embarrassing. *U.S. v.*
2 *American Optical Corp.*, 39 F.R.D. 580, 583 (N.D. Cal. 1966).

3 As the party moving to quash, Doe bears the initial burden of persuasion to
4 demonstrate that Kimberlite's requests are improper. *See Green v. Baca*, 226 F.R.D.
5 624, 653 (C.D. Cal. 2005). The burden on the party moving to quash is a "heavy
6 one." *Heat & Control, Inc. v. Hester Industries, Inc.*, 785 F.2d 1017, 1024-25 (Fed.
7 Cir. 1985). Doe's motion does not so much as attempt to meet this heavy burden,
8 but instead contains only two incompetent arguments regarding the complaint.

9 Doe's motion does not suggest that the documents sought are not relevant to
10 the action. There can be no question as to the relevance of the documents sought by
11 Kimberlite from AT&T. Kimberlite's email system was accessed without the
12 company's authorization by Doe. The true identity of Doe is obviously relevant to
13 the company's ability to prosecute its case against him. *See, e.g., Children's Legal*
14 *Services P.L.L.C v. Kresch*, 2007 WL 4098203 at *4 (E.D. Mich. Nov. 16, 2007)
15 (information that is relevant to identifying John Doe defendants named in complaint
16 is discoverable); *Wilkins v. Bittenbender*, 2006 WL 860140, * 7 (M.D. Pa. 2006),
17 (John Doe defendants are to be used until discovery allows plaintiff to determine
18 their true identities).

19 Similarly, Doe does not argue that the subpoena is improper. There is nothing
20 improper about Kimberlite's requests of AT&T. Kimberlite served a narrowly-
21 constructed subpoena upon AT&T Internet Services, asking only for information
22 sufficient to identify the individual who used the IP address 71.135.177.158 during
23 the times in which the initial two email break-ins occurred. Kimberlite has sought
24 nothing more than documents sufficient to reveal the name and address of defendant
25 John Doe—information necessary to serve process on him, prosecute the action, and
26 obtain an enforceable judgment against him. As such, nothing in this subpoena is
27 unreasonable or oppressive. Rather, it is simply an attempt to ascertain the identity
28 of the individual responsible for unauthorized network breaches. Unsurprisingly,

1 Doe sidesteps this issue entirely, and instead claims that "good cause exists" to
2 quash this subpoena because the CFAA is inapplicable, and his identity is protected
3 by the CPAA. Each of these arguments is entirely without merit, and the Court
4 should therefore deny Doe's Motion.

5
6 **II. DOE'S MOTION TO QUASH SHOULD BE DENIED BECAUSE**
7 **KIMBERLITE HAS PROPERLY PLEADED A CLAIM UNDER THE CFAA**
8 **AND FOR TRESPASS TO CHATTELS**

9 Doe offers no relevant legal support for his Motion to Quash. His arguments
10 repeatedly misinterpret the two statutes he does cite. Here, Kimberlite need only
11 show that there is a "real evidentiary basis for believing that the defendant has
12 engaged in wrongful conduct that has caused real harm to the interests of the
13 plaintiff." *Highfields Capital Management L.P. v. Doe*, 385 F. Supp. 2d 969, 970
14 (N.D. Cal. 2005). That is precisely what Kimberlite has done in its complaint.

15
16 **A. Kimberlite Has Satisfied All Elements to Establish A Cause Of**
17 **Action Under The Computer Fraud And Abuse Act**

18 The CFAA provides a civil remedy for damages or injunctive relief to "[a]ny
19 person who suffers damage or loss by reason of a violation of this section." 18
20 U.S.C. § 1030(g). Contrary to Doe's claims, a defendant need not access a computer
21 belonging to the United States or information belonging to the federal government
22 in order to be in violation of the CFAA. Indeed, CFAA Section 1030(a)(4) provides
23 the basis for a private plaintiff to bring a civil action. To succeed on a civil claim, a
24 plaintiff need only prove that (1) the defendant knowingly accessed a protected
25 computer; (2) the defendant did so either without authorization or by exceeding
26 authorized access; and (3) over the course of one year, the plaintiff suffered losses in
27 excess of \$5,000.00. 18 U.S.C. § 1030(a)(5)(B)(i), (g); *Physicians Interactive v.*
28 *Lathian Systems Inc.*, 2003 WL 23018270, at *6 (E.D. Va. Dec. 5, 2003). A

1 computer is a "protected computer" within the meaning of the statute if it "is used in
2 interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).

3
4 **B. Doe Knowingly Accessed Kimberlite's Computer Network Without**
5 **Authorization**

6 To establish the element of intent to defraud under the CFAA, the Court need
7 only find that the "defendant participated in dishonest methods to obtain" the data
8 from the protected computer. *Shurgard Storage Ctrs. v. Safeguard Self Storage,*
9 *Inc.*, 119 F. Supp. 2d 1121, 1125-26 (W.D. Wash. 2000). Plaintiff need only show
10 proof of wrongdoing. As plaintiff has pleaded, and as evidence indicates, this
11 requirement has been satisfied here. Doe, without authorization from Kimberlite or
12 the individual employees affected by his actions, logged into several Kimberlite
13 email accounts, and while there, viewed business-related emails intended for parties
14 other than Doe. (*See* Deedon Decl. at 1; Exhibits C, D.)

15 Doe's claim that he "has not had any intent and committed any fraud" is
16 absurd. On multiple occasions, he purposefully logged into password-protected
17 email accounts belonging to people other than him in order to view confidential
18 messages that were not intended for him. (Exhibits C, D.) As Doe accessed
19 information on Kimberlite's email system through dishonest means, Kimberlite has
20 satisfied its burden of showing wrongdoing.

21
22 **C. Kimberlite's Email System Was Used In Interstate Commerce And**
23 **Was Therefore A Protected Computer**

24 The CFAA defines a protected computer as one which "is used in interstate or
25 foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). Kimberlite's
26 computer network is used to conduct business and communications both inside and
27 outside of California. (Patterson Decl. at 1.) For example, Kimberlite has provided
28 service to dozens of military bases located in various states. (*Id.*) The Company

1 buys its equipment from companies located in several states and Canada, and as a
2 Sonitrol franchise, regularly communicates and conducts business with Sonitrol
3 Corporation, which is located in Pennsylvania, and Sonitrol affiliates located
4 throughout the United States. (*Id.*) Kimberlite is also in regular contact and does
5 business with customers who are headquartered outside California but do business
6 within the state. (*Id.*) In short, Doe's assertion that Kimberlite's computer network
7 is not a "protected computer" under the CFAA is baseless.¹

8
9 **D. Kimberlite Has Suffered Significantly More Than \$5,000 In Loss**

10 In determining the amount of losses suffered by a plaintiff as a result of a
11 violation of the CFAA, courts consider financial injury relating to "any reasonable
12 cost to any victim, including the cost of responding to an offense, conducting a
13 damage assessment, and restoring the data, program, system, or information to its
14 [prior condition]." 18 U.S.C. § 1030(e)(11). Among the costs that may be included
15 are "allegations of cost to investigate and take remedial steps in response to a
16 defendant's misappropriation of data." *Modis Inc. v. Bardelli*, 2008 WL 191204, at
17 *4 (D. Conn. Jan. 22, 2008).

18 Kimberlite has incurred losses of well over \$5000 in direct response to Doe's
19 unauthorized breach of its internal computer network. After discovering the
20 breaches, Kimberlite began an extensive investigation of its internal computer
21 network that is still ongoing. (Patterson Decl. at 1.) Among other things,
22 Kimberlite's IT personnel dedicated significant man-hours to ascertain the extent of

23
24 ¹ Moreover, a number of courts have held that transmission of data over the internet is
25 tantamount to moving the information physically through interstate commerce. *See U.S. v.*
26 *Carroll*, 105 F.3d 740 (1st Cir. 1997) (holding that transmission of photographs via the internet is
27 tantamount to moving them through interstate commerce); *U.S. v. MacEwan*, 445 F.3d 237 (3d
28 Cir. 2006) (holding that connection to a web cite or server must involve data moving in interstate
commerce). Thus, the computer was clearly one which was used in interstate commerce, thereby
qualifying as a protected computer within the CFAA.

1 the breach and protect against future breaches. (*Id.*; Deedon Decl. at 1) Remedial
2 measures were taken to secure the network, which required significant contributions
3 of personnel and equipment. (*Id.*) Moreover, the company incurred legal fees
4 because it had to retain outside legal counsel in connection with the investigation.
5 (Patterson Decl. at 1.) The Company also enlisted the help of private investigators
6 and forensic computer analysts. (*Id.*) These costs easily satisfy the requisite \$5,000
7 threshold. (*Id.*)

8
9 **E. Kimberlite Has Satisfied All Elements to Establish A Cause Of**
10 **Action For Trespass To Chattels**

11 In Doe's Motion to Quash, Kimberlite's cause of action for trespass to chattels
12 in completely ignored. To prevail on a cause of action for trespass to chattels, the
13 plaintiff need only demonstrate that the defendant, without authorization,
14 intentionally interfered with the plaintiff's rights in personal property, and that the
15 unauthorized use caused damage to the plaintiff. Courts have held that unauthorized
16 use of a plaintiff's computer is sufficient to establish damage and that no showing of
17 physical harm or substantial interference is necessary. *See Oyster Software v.*
18 *Forms Processing*, 2001 WL 1736382 (N.D. Cal 2001). As noted, *supra*,
19 Kimberlite has pleaded that Doe, without authorization, knowingly interfered with
20 Kimberlite's computer network, causing significant damages. This provides yet
21 another basis as to why good cause exists to grant the requested subpoena.

22
23 **III. THE CABLE COMMUNICATION POLICY ACT OF 1984 DOES NOT**
24 **APPLY HERE**

25 Lastly, Doe argues that the Cable Communication Policy Act of 1984
26 ("CCPA") does not allow operators to disclose personal data to third parties without
27 consent. However, the CCPA applies only to companies which "provide[] cable
28 service over a cable system" or a company which controls such systems. 47 U.S.C.

1 § 522(5)(A). The term cable service means any service which "includes the
2 transmission of local television broadcast signals." 47 U.S.C. § 522(2). The CCPA
3 was passed to "establish franchise procedures and standards which encourage the
4 growth and development of cable systems" and to assure the needs of the local
5 communities are served. 47 U.S.C. § 521(b)(2). Here, AT&T Internet Services
6 provided broadband internet access to Doe. AT&T operates a DSL network, and all
7 the data Doe illegally accessed was passed to him through telephone lines—not
8 cables transmitting television signals. The CCPA is wholly inapplicable in the
9 present context, in which an individual breached an internal computer network to
10 gain access to confidential information. Contrary to Doe's wishful assertion, the
11 CCPA does not protect, immunize or insulate Doe's wrongful conduct here.

12 Additionally, Doe's assertion that he maintains an interest in keeping this
13 particular information private is without merit. As an AT&T customer, Doe waived
14 any rights per his terms-of-use agreement.² Moreover, Doe's assertion that he
15 somehow has the right to spy on others' email and rummage through a company's
16 computer system, and invoke this Court's power to maintain the secrecy of those
17 actions is, of course, absurd. The sole issues here are whether Kimberlite served a
18 valid subpoena on AT&T, and whether Kimberlite has demonstrated sufficient
19 harm. Doe does not address the first issue, and with respect to the second his
20 arguments are purely speculative and without merit.

21 22 Conclusion


23 For reasons stated herein, Doe's Motion to Quash should be denied.

24
25 ²AT&T's own privacy policies expressly acknowledges that the company may,
26 without an individual's consent, provide personal identifying information to third
27 parties to comply with subpoenas, *available at* <http://www.att.com/gen/privacy-policy?pid=2506>.

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

DATED: May 16, 2008

QUINN EMANUEL URQUHART OLIVER &
HEDGES, LLP

By 
Scott G. Lawson
Attorneys for Kimberlite Corporation