IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF
VIRGINIA

PATRICK COLLINS, INC.,

Plaintiff,

vs.

DOES 1-58,

Defendants.

_____/

CASE No. 3:11-CV-531

MOTION TO QUASH OR MODIFY SUBPOENA (Does 1- 58)

"Notice to add additional argument regarding Motion to Quash or Modify Subpoena Dated 9/19/2011 (re: number 7 motion)"

MOTION TO QUASH OR MODIFY SUBPOENA

ADDITIONAL ARGUMENT

The attached study was prepared by the Computer Science Department at the University of Washington. This information will eventually be used in any trial of Doe defendants regarding P2P File Sharing and Copyright violations identified by only IP addresses. I respectfully feel the Courts should be aware of this study and it should be included in my argument to Quash or Modify. The Court should require the Plaintiff to identify each individual Doe using identification which can be proved reliable in the Court. Furthermore the Court should require the Plaintiff to identify the methods used to track down the thousands of IP addresses and these methods should include the source code used in any computer program, the program itself, the origin of the program and the error rate of IP addresses obtained in using this methodology.

Additionally the Courts should require the Plaintiff to divulge the shake down methods used in this case for collections and the collection amounts received. In the interest of transparency the Plaintiff should divulge the percentage of cases he can settle without trial, the amounts of these settlements and the total costs involved to the Plaintiff. It is without question unfair for a Lawyer to use these methods which cost little and end up costing thousands of dollars to innocents all over the United States.

In my case it is impossible for the Plaintiff to prove my guilt. My case involves a business, which was unoccupied at the time stated on the Subpoena, it involves computers which have been subjected to malware numerous times, it involves security cameras used for surveillance purposes to secure legally proctected data and it involves printers, network drives used to backup data, network dvrs to record surveillance and equipment which cannot be secured against those

who have the knowledge to spoof it or hack into it, just as many large financial, military and educational institutions have found time and time again. Hardly a day goes by that the news does not contain a story where a computer system containing highly confidential data has been hacked, spoofed and infected by malware. Until the system can overcome all these issues these so-called IP Doe cases should be dismissed until the burden of Proof is on the Plaintiff and not the defendant. The defendants in many of these cases are underage, elderly, businesses, educational and governmental institutions. In one of these cases the defendant was the computer repairman for the Plaintiff's attorney.

Respectfully submitted,

John Does 1- 58

s/John Does 1-58
John Doe
Pro se

Attachment includes

The University of Washington paper titled "Challenges and Directions for Monitoring P2P File Sharing Networks –or- Why my Printer Received a DMCA Takedown Notice"

CERTIFICATE OF SERVICE

I hereby certify that on 10/13/2011, I served a copy of the foregoing document, via US Mail, on:

D. Wayne O'Bryan, Esquire
1804 Staples Mill Road
Richmond, VA 23230