Harmony Oswald

IP Theory

**The Unheightened Reality of Plausibility Pleading**

*Identification of Defendants in Copyright Infringement Claims Using Only an IP Address Impacts Hundreds of Thousands*

Internet Protocol account holders beware:

Since 2010, hundreds of thousands of individuals have been sued for copyright infringement based upon their IP address alone.1 Under the *Twombly* plausible pleading standard, a complaint must contain enough factual matter, taken as true, to raise the right to relief above a level of speculation where one outcome is just as likely as another.2 A pleading must be based on more than mere suspicion or conclusory allegations, and it must include contextual facts to support a theory that discovery will reveal evidence of illegality.3 Still, claims based on nothing more than alleged infringement associated with a particular IP address continuously move forward. Worse, often times allegations include the illegal distribution of pornographic content.4

The trend in most courts is to allow an IP address to suffice to identify the defendant in pleading.5 This means that if a plaintiff's investigator determines the IP address where copyright infringement allegedly occurred, the plaintiff may use that IP address, without more, to identify the defendant. In these cases, the court accepts as plausible the theory that the person associated with that IP address is the same person that allegedly infringed plaintiff's copyright. With no direct evidence linking the physical person whose name is on the ISP account to the alleged copyright infringement, however, the pleading includes nothing more than a conclusory allegation. It is customary for a single IP address to be shared amongst family members, roommates, neighbors, and the like. Thus, it is just as plausible that the person named on the copyright infringement claim is *not* the party who infringed the copyright. Under the *Twombly* plausible pleading doctrine, when a proposed theory "could" be consistent with truth just as well as any other theory, the facts fall short of meeting the standard to move forward with the claim.6

A minority of courts have begun to view the situation differently. In an effort to protect innocent defendants, these courts refuse to allow an IP address to suffice to identify a defendant.7 The logic behind this argument is that a person who pays for the IP account is not necessarily the party who engaged in the alleged copyright infringement. With access to wireless routers a prevalent reality of the times, various individuals may access the IP address from inside the home, or even outside of the home.

In this paper, I will argue that changes in procedural policies with regard to copyright enforcement are necessary to establish uniformity of laws. I will take the minority view that an IP address alone does not accurately or adequately meet *Twombly* plausible pleading standards. If, however, it is still desirable and necessary for an IP address to suffice to identify a defendant in copyright infringement pleading, then Congress should enact a "duty to secure" law to provide notice to the public of legislative intent, and to reduce the likelihood that an innocent defendant will be named a party to a copyright infringement lawsuit. Alternatively, courts should adopt the minority approach by refusing to allow an IP address alone to identify a defendant. I will provide support for the theory that freeing the market could enhance public interest without negatively impacting the incentive to create.

This discussion is organized into three parts. Section (A) describes the current state of affairs regarding rampant online piracy and mass copyright infringement lawsuits. Section (B) discusses Federal Rules of Civil Procedure, modern *Twombly* plausible pleading standards, and the problems associated with and specific to online copyright infringement lawsuits where identifying a defendant is impossible unless an IP address is used. Section (C) evaluates two ways courts are approaching the issue. A majority of courts take the position that necessity mandates allowing pleading in copyright infringement claims to identify an alleged infringing party with an IP address alone. A minority of courts refuse to allow this procedure where plausibility standards in pleading are not met. I will discuss two alternative solutions to the problem. Either (1) pleading using an IP address should be allowed, and Congress should enact a "duty to secure" law to notify the public of this procedure, or (2) in absence of such legislation, courts should not allow pleading using an IP address. Either way, the public interest will be served, as discussed below.

**A. CURRENT STATE OF AFFAIRS**

Digital piracy is generally rampant, and piracy of pornography tops the list.8 Although over 70,000 jobs and 2.7 billion in earnings are lost in the U.S. each year due to online piracy, 70 percent of online users find nothing wrong with stealing content.8 As a result, copyright owners file thousands of copyright infringement lawsuits each year, and many against users of BitTorrent software.14 BitTorrent is not an evil in itself, but instead addresses inefficiencies associated with traditional file sharing.13 It makes the file sharing process much more effective and efficient.

Under the standard client-server model, huge digital files are distributed to a large number of people from a limited number of computers.13 Since the files tend to be in high demand, a heavy load is placed on the limited source computers and their associated bandwidth.13 This causes the distribution process to be slow.13 BitTorrent is one of several peer-to-peer file sharing protocols that address this problem by allowing users to obtain a copy of the large file and to become an additional source, or "seeder."13 The seeder's software divides the large file into thousands of smaller files.13 Each piece is given a 40 character alpha-numeric code, or "fingerprint."13 The BitTorrent software creates an associated ".torrent" file which includes information about the original, the tiny pieces, and the digital fingerprint code.13 The seeder posts the .torrent file to a host website. When other BitTorrent users are ready to download a copy, they search the Internet using a torrent search engine to find a file of interest.13 Once a file is downloaded, another "tracker" computer running BitTorrent software locates a swarm of peers sharing pieces of the particular file described by the torrent file.13 Additional downloads may be from any peer that has already downloaded a segment of the specific file.13 The BitTorrent software automatically offers any piece of a digital file previously downloaded to the group.13 The software checks authenticity by verifying the fingerprint.13 Once the BitTorrent user downloads every necessary piece, the software rearranges the file into a single, viewable movie.13 Peers continuously share among small groups, and over the long run may be involved in sharing with thousands in the swarm.13

There is no U.S. government enforcement agency tasked with policing copyright infringement.9 According to Ben Depoorter, a professor at the University of California, Hastings College of Law, the law is designed primarily for private civil lawsuits.9 In the same way that music labels banded together to hold Napster accountable in the past, movie studios are currently filing mass lawsuits against Bit Torrent users.10 For example, this year, Malibu Media, a pornographic film company based in Southern California, filed nearly 40 percent of all copyright claims.9 In 2013, Elf-Man LLC, a small independent movie company that produced the Christmas movie *Elf-Man,* sued several hundred alleged infringers.11 Voltage Pictures, the studio that created the film *The Hurt Locker*, sued nearly 25,000 individuals for copyright infringement in 2011.10 That same year, Nu Image sued 23,000 individuals for allegedly downloading *The Expendables*.1

Plaintiffs typically initiate an investigation where forensic software is used to identify IP addresses associated with use of BitTorrent protocol to reproduce, distribute, display or perform works.13 The query usually reveals a list of IP addresses and related information which is attached as an exhibit to the complaint, to provide factual support for the infringement claim.13 The information includes the Internet Service Provider responsible for assigning the IP address at issue, a date and time when the alleged infringement occurred, and the city and state where such activity occurred. The plaintiff then files a claim and makes a motion for leave to serve a third party subpoena on the ISP provider prior to the FRCP 26(f) conference.13 The purpose of the subpoena is to secure the name of the individual assigned the IP address, the residential address (to aid in jurisdictional analysis), email address, and Media Access Control address for that individual.13

Routers with a single IP address, however, are often shared among multiple computer users. When a wireless router is not secured, neighbors, visitors, family members, or passersby may access the IP address. This makes it difficult to pinpoint the exact individual who committed an illegal act. Even with security measures in place, a tech-savvy individual could bypass security to use the targeted address. More problems arise when a business is involved. Employees, customers, or members of the public could be involved in illegal distribution of copyrighted material. Some estimates conclude that approximately 30 percent of the names turned over by ISPs are not those of individuals who actually downloaded or shared copyrighted material.12 Since an IP address does not precisely identify the party involved in copyright infringement, the situation creates a risk of bringing innocent parties into litigation.12 This may waste valuable court resources and place an undue burden on the IP addressee. Thus, opinions vary regarding whether this type of discovery and questionable procedural tactic should be permitted.12

**B. PLAUSIBILITY PLEADING**

In order to sufficiently state a claim under FRCP 8(a)(2), the law requires a plaintiff to offer a "short and plain statement . . . showing that the pleader is entitled to relief," in order to "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests."21 To determine whether identifying a defendant with an IP address meets current pleading standards to survive an FRCP 12(b)(6) motion to dismiss, courts should apply the rules set forth in *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007).16 In that case, subscribers to local telephone and Internet services filed a claim against carriers, alleging that they were engaging in "parallel conduct" constituting a restraint on competition in violation of the Sherman Act.15 The issue was whether the factual context in the pleading met the standard to survive a motion to dismiss.15 The Court reviewed and updated the standard set out in *Conley v. Gibson*, which held that any statement revealing the theory of the claim would suffice unless it was a factual impossibility.15 Under the old approach, a conclusory statement would survive a motion to dismiss whenever the pleading left open some possibility that a plaintiff might later establish facts to support recovery.17 This was true even when the complaint did not set forth a single contextual fact that suggested the elements of the claim were met.17 In *Twombly*, the Court stated that *Conley* was never interpreted literally, and that a complaint must contain either direct or inferential allegations respecting all material elements essential to sustain recovery under a viable legal theory. 17 The Court rejected the view that courts have a duty to imagine unpleaded facts that might secure a cause of action.18 Instead, the Court held that for a pleading to survive a motion to dismiss for failure to state a claim, a plaintiff must offer factual support consistent with the allegations in the complaint, to meet the heightened standard of "plausibility."18

When considering whether a pleading sufficiently alleges a clear violation of law, a court must consider whether the facts meet the elements required by the law to establish a violation.19 For example, to state a claim for copyright infringement, a plaintiff must first establish ownership in a valid copyright.20 Next, plaintiff must offer factual support showing that the defendant violated one of the exclusive rights the copyright owner holds in the work.20 The facts must (1) provide the specific work in issue, (2) show that the plaintiff owns the copyright for that work, (3) show that the copyright for that work is registered in accordance with statute, and (4) describe what acts the defendant engaged in and during what time to infringe the copyright.20 Conclusory allegations that an infringement occurred will not suffice to meet the *Twombly* standard for plausibility pleading, and are not entitled to an assumption of truth when a court considers a motion to dismiss for failure to state a claim.20

Probability is not required, but enough facts must be asserted to raise a reasonable expectation that discovery will reveal evidence of illegality.21 The statement must cause the factfinder to do more than speculate that a claim might have merit.21 Further, the claim should suggest more than consistency that the events could have occurred as suggested.21 If another theory could be offered that is just as likely, the standard is not met.21 Even where the circumstantial evidence is otherwise admissible, the court does not take the step to make overbroad inferences unless the evidence adequately excludes other possibilities and explanations.22 The requirement for stating grounds for entitlement to relief means that a plaintiff must offer more than conclusions, labels, or bare assertions that the elements of the cause of action are met.21

In *Twombly*, the Court analyzedthe complaint by applying a two-pronged approach, to determine whether the facts alleged were (a) plausibly stated, assuming their veracity, to suggest (b) entitlement to legal relief.24 The plaintiff had flatly pleaded that the defendant entered into a conspiracy agreement to prevent competition.24 The facts alleging an agreement in violation of the Sherman Act were conclusory, and were therefore not granted an assumption of truth.24 Thus, where the elements of the cause of action were not met and entitlement to legal relief was not shown, the Court granted the motion to dismiss for failure to state a claim.25

The policy behind the plausible pleading rule is to prevent meritless or unprovable claims from moving forward and taking time and resources away from the court and other people.23 When the allegations in a complaint do not support a plausible claim for entitlement to relief, the court should act immediately to dismiss the claim, to prevent unnecessary expenditures.26 Discovery can become extremely costly, and may account for as much as 90 percent of litigation costs when actively employed.27 Due to the threat of discovery and other litigation costs, cost-conscious defendants often settle cases that are without merit. Further, when copyright infringement of pornographic film is involved, defendants may settle to avoid embarrassment. For these reasons, a district court must retain the power to insist upon some specificity in pleading before allowing a claim to proceed.28

**C. SPLIT IN AUTHORITY**

**1. The Majority Approach**

Recently, copyright litigation involving the BitTorrent file-sharing protocol has proliferated, and has been the subject of lively debate in the judicial system and across the internet."37 The BitTorrent tracking feature makes it possible for individual plaintiffs to identify the IP address where copyrighted films were downloaded.29 The IP address is easily identified by a numeric label specific to the computer network that serves to identify and locate the network on the internet.29 Identifying the exact user, however, is not so easy.29 Thus, it is commonplace for a plaintiff to identify a defendant in a copyright infringement pleading strictly by naming the IP address where copyright infringement took place.29 Theplaintiff immediately files a motion for leave to serve a third party subpoena on the Internet Service Provider affiliated with the alleged infringement, requesting the name, address, phone number, and email address of the account holder associated with the IP address listed on the complaint.29

An ongoing question among courts is whether a copyright infringement claim filed against an IP address based solely on the fact that the defendant owned such IP address meets the plausible pleading requirement set forth in *Twombly*.30 More specifically, a court must review whether a plaintiff has properly included facts stating by what acts and during what time the defendant infringed the copyright in issue.31 The majority of courts find that a pleading is sufficiently plausible where the alleged copyright infringement claim is based on BitTorrent technology and the defendant is identified solely based on an IP address.32

For example, in *Patrick Collins, Inc. v. Doe 1*, the court denied the defendant's motion to dismiss for failure to state a claim where plaintiff included relevant BitTorrent details alleging that the defendant installed the Client onto his computer, and accordingly alleged a belief that the defendant went to a torrent site to upload and download the plaintiff's copyrighted work.33 The court stated that the plaintiff adequately pled a plausible claim by providing sufficient details about the acts the defendant took to infringe.33 In *John Wiley & Sons, Inc. v. Doe Nos. 1-30*, the court found that the plaintiff made an adequate showing of prima facie copyright infringement by claiming ownership of the copyrighted material Windows 7 Secrets, and offering specific details regarding the alleged unlawful copying and distribution of the work, including dates and times when infringement occurred, the file sharing protocol used, and the IP address of the computer onto which files were copied.33 In *Braun v. Primary Distributor Doe,* a plaintiff alleged that a computer using the IP address assigned to the defendant participated in the alleged infringing activity.34 The court found that the complaint was sufficient despite the defendant's argument that the allegations were speculative and conclusory and did not meet plausible pleading standards since the claim was not filed against an individual person.34 The court reached a similar finding in *Elf-man, Inc. v. Does*, where the plaintiff provided the IP address assigned to each Doe defendant, the date and time of the download at issue, the hash identifier, the ISP, and the location of the IP address on the pleading.35 The complaint survived a motion to dismiss and the court found the complaint stated the allegations with sufficient specificity.35 The court compared the situation to *Arista Records*, where defendants engaged in anonymous online behavior that would likely remain anonymous unless the plaintiff was permitted to ascertain the identities via expedited discovery.36

Individualsnamed on a complaint by their IP address tend to find fault in the process. A defendant will often file a FRCP 12(b)(6) motion to dismiss for failure to state a claim, arguing that the sole fact that an individual pays for Internet service and is issued an IP address is not sufficient factual support to heightened plaintiff's theory of copyright infringement from one of possibility and mere conjecture to one of plausibility. When considering a motion to dismiss pursuant to FRCP 12(b)(6), the issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims.39 The court accepts all factual allegations in the complaint as true, and makes all reasonable inferences in plaintiffs favor.39 The court may refer to documents attached to the complaint as an exhibit, those plaintiff relied upon in bringing suit, and reference matters of which judicial notice may be taken.39 A complaint must plead enough facts to state a claim that is plausible on its face.39 Only if the court is satisfied that the complaint cannot state any set of facts that would entitle the plaintiff to relief will it grant dismissal pursuant to FRCP 12(b)(6).42

As the District Court for the Eastern District of New York explained, although there may be doubts that the subscribers of IP addresses are actually the individuals who infringed the copyright, difficulty in proving guilt is not relevant in the context of a motion to dismiss.40 A reasonable possibility that the defendant did not infringe the copyright and another individual did matters not when it is an equally reasonable possibility that the defendant did commit the alleged act.40 The court in *Twombly*, however, stated that a theory must go beyond "consistency" where another theory would be just as likely, and must include evidence to exclude the alternatives.41

Nevertheless, under the majority approach, a pleading using only an IP address to identify the defendant is found to meet the standard under FRCP Rule 8 requiring that acts associated with alleged copyright infringement be stated with some specificity.38 This method of identification is deemed to satisfy element (4) of the basic test applied to establish a copyright infringement claim where, as a general matter, a plaintiff must state in the pleading (1) what particular works are the subject of the claim, (2) that the plaintiff owns the copyright in those works, (3) that the works are registered in accordance with statute, and (4) *by what acts and during what time the defendant infringed the copyright*.38

Although an investigation revealing a particular IP address associated with copyright infringement provides information about location, time, what activity took place, and the connection used, and although further information from an Internet Service Provider may lead to the name of the account holder who pays for the service, it does not reveal with any specificity who took the action. Although it is possible that the person whose name happens to be on the account of an IP address that was used to engage in the conduct is the same person who took the illegal action, alternative parties are in no way excluded. It could just as likely be the neighbor, a guest of the neighbor, a teenage daughter, the son's friend who visits every Saturday, or Aunt Edna who came over for Thanksgiving dinner who used the IP address in question to engage in the alleged acts. Thus, arguably, identifying a defendant using an IP address alone does not adequately meet *Twombly* plausible pleading standards.

If, however, reasonable policy concerns such as necessity or dissolving rampant piracy require that citizens who contract for an IP address be held accountable to answer for all activities occurring at such address by allowing such address to "quasi-identify" a defendant in a copyright infringement pleading, Congress should enact a law to explicitly provide notice to the public regarding rights, obligations, and legislative intent. Citizens should be well informed and equipped to take precautionary measures to reasonably secure technology within their control, that they might guard themselves against the hardships and pressures associated with legal action against them. The flexible approach of "judicial policing" of the Internet does not provide adequate uniformity, consistency, or fairness in an area of the law where hundreds of thousands of citizens are currently being identified by their IP address, there's arguably high risk that innocent parties are named, and most defendants are settling outside of court to avoid high legal fees and embarrassment associated with being named on a suit.9

**Proposed Solution: Explicit "Duty to Secure" Legislation**

*If an IP address should suffice to "quasi-identify" the defendant in a pleading, then Congress should enact legislation to explicitly codify the pleading procedure. The law should provide that a party who contracts for an IP address may be identified by such in a pleading of or related to copyright infringement occurring at such IP address.*

***Importance of Congressional Codification***: Laws reflect the intellectual, social, economic, and political climate of the times and are inseparablefrom the interests, goals, and understandings that shape social life.43 Discussions regarding the law often debate whether the law effects society, or society effects the law.44 The answer is likely both. For example, many scholars contend that a principal function of law in modern society is social engineering.45 On the other hand, the Law and Society perspective of purposive, planned, and directed social change initiated, guided, and supported by law is similar to Legal Realism in that it treats law not as a closed system of internalized logic, but as the product of great external influences, like power, history, and social, economic, and cultural exchanges.44 When Holmes proclaimed "the life of law has not been logic, it has been experience," he was attacking the internalistic perspective that led to false certainty due to confusing legal reasoning with mathematical or geometrical formulas.44 Roscoe Pound's Sociologic Jurisprudence also heavily influenced the Law and Society movement.44 Pound regarded law as a social institution to satisfy the claims and demands of a civilized society by applying social control efficiently and effectively to eliminate waste and preclude friction to maximize human enjoyment of goods.45

Regardless of the exact interplay between society and its laws, it is widely accepted that in a complex heterogeneous culture, explicit regulation through enactment of a working system of formal and universal legal rules to govern commercial transactions and other scenarios is necessary to ensure predictability, continuity, and effective methods for settling disputes.46 Advancements in civilization continuously raise the need for development of new laws.46 The most widely accepted theory of lawmaking is the rationalistic model, which advocates creating law to protect society from social harms.47

To meet this purpose, legislative action is most effective. Judge made law provides no rules in advance, and is based on decisions courts make about actual controversies based on justifications for applying certain rules to specific facts unique to each case.48 Legislators, on the other hand, formulate rules providing advance notice to society about what is required, what is authorized, and what is prohibited, in anticipation of situations that will likely arise.48 In addition, legislators are charged with responding to specific problems and addressing new technological innovations that impact a numerosity of individuals.48 When new problems emerge, the probability of new legislation increases; especially when the public is unorganized, intensely concerned, and there is no pressure to maintain the status quo.49 The stages of developing new legislation typically include (1) publicity and instigation by the media (present stage), (2) researching costs, benefits, inherent difficulties, and political impact, (3) formulation of the law, and (4) obtaining support for the law.49

In the current state of affairs, where copyright owners are filing mass lawsuits using only an IP address to identify a defendant in pleading, the law is lagging behind the social change that occurred. The Internet created a new problem in identifying parties. Without formalized legislation, courts are left to decide on a case by case basis whether an IP address should suffice to meet the standard set forth in *Twombly*. The need for legislation is readily apparent when noting the amount of time and resources being allocated in thousands of cases where judges must evaluate whether an IP address meets the pleading doctrine. Courts are left to weigh the harm done to the plaintiff (where necessity mandates using an IP address for identification) with the harm done to the IP address account holder in the reasonably possible event that the account in question was used by a third party. A majority of courts are allowing identification with an IP address to suffice, in order to enforce the copyright in question. If this outcome is desirable, legislation is necessary to ensure predictability, continuity, and effective methods for dispute resolution. As it stands, citizens have no way of knowing about the implicit "duty to secure" that follows when they contract with an ISP provider. Fairness mandates legislative action where huge numbers of citizens are impacted, and many are settling outside of court to avoid legal fees or being named on questionable suits.9

***Social Control and Effect of Codification:*** In various contexts, law functions to promote social change, to facilitate dispute settlement, and to provide social control.50 Social control refers to the methods used to maintain order and promote predictability of behavior among citizens in a society.52 In a heterogeneous society such as the U.S., social control largely rests upon internalization of shared behavioral norms.53 Most individuals behave in socially acceptable ways due to fear of disapproval from family, friends, and neighbors upon deviation.54

There are two aspects involved with social control.55 The first, internalization of group norms, occurs where an individual develops self control by being educated regarding appropriate, expected, or desirable behaviors in certain contexts.55 Here, people are motivated to conform to norms simply because "they should," regardless of anticipatory reactions of others.55 The other type of social control occurs via external public pressure from laws that gain compliance by means of positive and negative sanctions.55 External public pressure may also lead to internalization of shared behavioral norms. This exemplifies the interaction between law and society.

Formal legal mechanisms for social control are most necessary in environments where the population is diverse, and in situations where values, attitudes, and socioeconomic standing creates disparities.51 Explicit rules, standard procedures, predictability of universal sanctions, and designated officials to interpret and enforce rules are desirable.51 These social institutions are organized for securing conformity to socially desirable behaviors and consists of established compulsive procedures to best satisfy human needs.56

The Internet provides access to a world-wide community where there is sparse commonality among users. This creates an environment where calculated formal legal mechanisms may benefit society. Since online copyright infringement lawsuits are currently prevalent and the majority of courts allow an IP address to identify the defendant in pleading, explicitly codifying the pleading process will establish predictability and uniformity of laws. Individuals will be informed regarding expectations under the law, in order that they might conform to socially desirable conduct. As a result, innocent parties will be better protected. The likelihood that an IP address account holder is incorrectly identified as the person who engaged in copyright infringement might reasonably decline as more users become aware of obligations with respect to Internet security, and are educated regarding protecting themselves against frivolous lawsuits. Over the long run, shared behavioral norms will likely develop as people teach each other about the explicit duty to secure under the law. Responsible behaviors with regard to Internet security may become customary.

***Policy of Individual Responsibility:*** As it stands, hundreds of thousands of individuals are being impacted by decisions to allow "quasi-identification" using no more than an Internet Protocol address.66 There is an assumption in the majority of courts, therefore, that an individual who contracts with an Internet Service Provider should be held accountable to answer in court for activity that occurs at such address.

To understand this line of reasoning, it is helpful to think of an IP address as similar to a real address.57 Each IP address has ports, or "doors of entry" associated with it.57 Even if someone arrives at the address and goes in the door, they can only interact in one room unless granted permission to access the rest of the building.57Importantly, if an intruder (or potential copyright infringer) knows the address, this does not create a problem.57 What matters is whether security is in place to deter a break-in where a third party could potentially use the premises for unlawful conduct.57 Without security, the network is a target for exploitive conduct.57 An unsecure network is open to the public, and the public activities will be traced back to the unsecured network's residence.57 The IP addressee could be charged for conduct not directly committed by him/her.57 By taking steps to secure Wi-Fi networks, citizens and their data are protected from unwanted attacks and frivolous lawsuits, and minors are protected from harmful content as well.57 Implicit in the majority view is the assumption that every IP addressee should ensure that his/her IP address is configured securely, patched, and limited.57

The duty to secure an IP address is also comparable to the duty to secure a vehicle by taking the keys out of the ignition. When keys are left in the ignition, the owner of the vehicle invites another to use it, and as a result, the vehicle could be used to commit unlawful acts. For example, in *Cruz v. Middlekauf Lincoln-Mercury*, 909 P.2d 1252 (1996), a car dealership's management policy included leaving keys in the ignition of vehicles. A thief stole one of the vehicles, and crashed into another vehicle, causing injuries.58 The injured party sued the owner of the car dealership for damages.58 The court held that defendant's motion to dismiss for failure to state a claim was properly denied where defendant left the keys in the ignition, and engaged in other activities that significantly increased the likelihood of the criminal conduct.58 Thefts often occurred in this manner, the public had unlimited access to the cars, and still the defendant continued a management policy of leaving keys in the ignition.58 Thus, the conduct was foreseeable, and the intervening use of the car did not preclude a finding of proximate cause against the defendant.58

The case of the keys left in the ignition compares to failure to secure an IP address. By failing to secure, the owner of the IP address offers the public unlimited access to the Internet connection to use in countless ways. Piracy and other illegal conduct online is prevalent, and such conduct is more likely to occur at an unsecured address. Implicit in the majority view is the assumption that the person who contracted with an ISP provider for an IP address has a duty to secure that "vehicle." Thus, identifying a defendant by such address in a copyright infringement complaint will suffice to meet plausible pleading standards under *Twombly*.

***Imperfect Solution:*** A codification of the majority view to allow an IP address to suffice in pleading a copyright infringement claim is not a perfect solution on all points. One problem arises where the law will not impact the public if the public is left unaware of the law. A solution to this issue could be a requirement under law that ISP providers, at the time of contract, give notice to parties signing for an IP address of their rights and obligations under the law. The notification might include information such as how to reasonably secure technology, probability that an unsecured IP address is more likely to lead to use by third parties, and notice that the party contracting for the IP address may be identified in pleading and held accountable to answer in a court of law for any and all copyright infringement occurring at such address. An example of such public notification requirement can been seen in the similar process required of health care providers under HIPAA.59

Another concern involves the fact that codification will still not lead to perfect identification for pleading purposes. The defendant/IP address account-holder will nevertheless be afforded the opportunity to be heard and prove his/her innocence in a court of law. Many courts allow the defendant to remain anonymous as the case progresses toward trial or settlement, with names revealed only if a monetary judgment is ordered.9 Moreover, the public notification may decrease the overall likelihood of error by initiating individual security measures and increasing the amount of citizens protecting themselves.

Finally, a question arises regarding whether or not a duty to secure might create an undue burden, chill speech, or effect individual rights to anonymity. Courts find that Internet users do not have a reasonable expectation of privacy in their subscriber information such as name, address, phone number, or email address, when they have already conveyed this information to their ISP to set up an account.60 Further, the individual also has no reasonable expectation of privacy when the same unprivileged information is sought in a subpoena.60

When a file sharer is engaged in expression implicating First Amendment protection, the *Sony* test applies.61 Five factors should be considered in weighing the need for disclosure of the identifying information.61 There must be (1) a concrete showing of a prima facie claim of actionable harm, (2) specificity in the discovery request, (3) no alternative means to obtain the identifying information, (4) the information must be essential to advancing the claim, and (5) the party's expectation of privacy must be considered.62 First Amendment freedom of speech does protect the right to receive and view films on the Internet, but that right is not absolute, and certain classes of speech, such as libel, obscenity, and copyright infringement are not protected.60 The alleged infringement means the defendant's First Amendment rights are at a low ebb, and a general denial of illegal conduct does not change this fact.63 It may be true that the defendant did not engage in the illegal conduct, and perhaps the plaintiff will choose not to name the individual as a party, but most courts take the stance that quashing a subpoena would deny the plaintiff access to critical information necessary to bring these individuals properly into the lawsuit where exploration of the merits and testing the veracity of the defense is possible.64 Plaintiff's right to use the judicial process to pursue a prima facie copyright infringement claim trumps a defendant's right to freedom of speech, anonymity, or privacy.65 Thus, BitTorrent users may engage in expressive conduct by file sharing, but the *Sony* factors weigh in favor of disclosing the defendant's identifying information.62 The information is not "protected" when triggered by FRCP 45.60

**2.** **The Minority Approach**

Not all courts find that an IP address used to identify the defendant in a copyright infringement claim meets *Twombly* plausible pleading standards. Here, I will explore the minority's approach to pleading. Then, I will provide support for the theory that freeing the market could enhance public interest without negatively impacting the incentive to create.

On March 19, 2014, Florida District Judge Ursula Ungaro dismissed a case brought by Malibu Media against IP addressee 174.61.81.171.67 Rather than granting Malibu Media a subpoena to get records from the ISP, she issued an order to show cause asking why geolocation or other technology is reliable to prove that a defendant is located within the court's jurisdiction.67 After reviewing Malibu Media's response, the judge determined that although the geolocation software did establish a location for an IP address, Malibu Media did not show how this could prove identity since the IP address was not linked to an exact person.67 Thus, jurisdiction over the defendant was not established and the case was accordingly dismissed for improper venue.67

A few other courts agree that an IP address alone does not necessarily reveal much about individual conduct occurring at such address.68 For example, a court in New York found that the assumption that the account holder who pays the ISP is the same person who allegedly downloaded a single film is tenuous because an IP address provides only the location where countless computer devices may be connected.69 An IP address is comparable to a telephone number in a house with numerous telephones, and it is no more likely that the person paying for the IP address engaged in conduct on a computer at such address than it is that the person paying the telephone bill made a specific call.69 Over 60 percent of homes now have wireless access that can be freely accessed by numerous individuals.69 Thus, unless security measures are in place to aid in the identification process, it is inaccurate to assume with any level of certainty that the IP address account holder engaged in the copyright infringement.69

As many as 30 percent of identities provided by ISPs likely represent individuals who did not engage in the alleged infringement.70 By allowing identification in pleading using only an IP address, plaintiff's discovery has the potential to bring many innocent defendants into litigation.70 Further, the threat of high litigation costs may pressure innocent parties into unjust agreements, especially in copyright infringement claims where embarrassment associated with pornographic piracy motivates quick settlement.70 According to these courts, the undue burden involved weighs against allowing this method of creative pleading to proceed.70

A Washington court agreed with the minority approach.71 The filmmakers who created *Elf-Man* sued hundreds of people for allegedly pirating the film using BitTorrent.72 The court found that an IP address used to identify the defendant did not suffice to meet the pleading standard set forth in *Twombly*.72 The complaint failed to provide factual support to rule out the possibility that another party engaged in the conduct, or to show with clarity that it was plausible that the IP address account holder was the culprit.72 Plaintiffs alleged that the defendants either downloaded the film, or permitted, facilitated, or promoted others to use their IP address to do so.72 The court found this allegation insufficient since it only accused the IP address account holder of failing to secure the account.72 The court's statement suggested that account holders are not currently responsible for conduct of other parties using their unsecured account.72

As it currently stands, the minority approach to pleading makes copyright enforcement of online films impossible. Creative expression gets no copyright protection, and piracy runs rampant due to lack of policing methods. Eliminating the restriction of monopoly, however, means that freedom prevails. People are able to exercise individual rights in the open market of free-flowing ideas.

**Alternative Solution: Courts Should Not Allow IP Address Pleading**

***Internet Freedom Theory:*** From a theoretical perspective and under a normative approach, the minority of courts are getting it right. Online films do not neatly fit the mold for subject matter that should be taken out of the public domain and made subject to property ownership and copyright enforcement. Although films are often costly to make, cheap to copy, there is limited depletion of the commons, and low risk of inadvertent trespass, a huge problem arises where it is virtually impossible to identify with specificity who engaged in the trespassing activity. The barriers to proving infringement and the costs involved when innocent defendants are coerced to settle does not make a strong case for copyright enforcement in this area.

Although property rights may help move items to their highest valued use, in the market for online films little is lost when copyright is eliminated because history suggests that artists will create works anyway.74 Markets commonly thrive without intellectual monopolies.75 A useful model is the development of the computer industry beginning at the end of World War II.75 This is an example where innovation flourished without enforcement of intellectual property law.75 In addition, literature thrived for centuries in the complete absence of copyright, and many historic authors were never paid copyright royalties.80 Disney productions like Snow White, Sleeping Beauty, Pinocchio, and Hiawatha were all taken from the public domain.77 Even Hollywood itself developed due to piracy.78 Free entry and unrestricted imitation often precede success, while monopolistic restrictions may lead to poor subsequent economic performance.79

Some scholars view intellectual monopoly as a consequence of innovation, rather than an incentive for it.81 The idea is that intellectual property rights protect creators so that they are able to engage in old ways of doing business.81 A model of this theory becomes apparent when reviewing the history of Microsoft.81 In the beginning, Microsoft made little effort to prevent piracy of their software.81 As creative output declined over the years, effort to enforce intellectual property rights increased.81 A similar situation is apparent in various media outlets.82 Huge royalties become the norm in industries such as Hollywood film.83 Thus, the function of copyright law is not to provide incentive to create or improve.84 The goal is to maintain the status quo.84 Some courts adhere to the duty to guarantee such profits in the future, despite changing circumstances or competing public interests.84 Here, under the minority view, commitment to plausible pleading doctrine, protection of innocent defendants from coercive settlement tactics, and technological consciousness trump the duty to enforce copyright in online film.

***In Conclusion:*** Identifying a defendant in a copyright infringement claim using an IP address is permitted in the majority of courts. The tedious case-by-case analysis, however, leads some courts to question whether this creative tactic meets plausible pleading standards under *Twombly*. If "quasi-identification" is necessary to enforce copyright, Congress should codify the majority view by enacting a law to explicitly notify the public that a party who contracts for an IP address may be identified in a pleading for copyright infringement occurring at such address. Otherwise, courts should not allow an IP address to suffice where it is impossible to determine who engaged in copyright infringement activities at such address.

Works Cited

1 *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80 (2012);

2012 U.S. Dist. LEXIS 61447, \*82

2 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

3 *Id*.

4 *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D.80(2012); 2012 U.S. Dist. LEXIS 61447, \*82

5 2013 U.S. Dist. LEXIS 44131, \*4; 2013 U.S. Dist. LEXIS 66319, \*4

6 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 554 (2007).

7 *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80 (2012); 2012 U.S. Dist. LEXIS 61447, \*84; *Elf-Man, LLC v. Doe*, 2013 U.S. Dist. LEXIS 112128; *Malibu Media, LLC v. Doe*, 2014 U.S. Dist. LEXIS 82480

8 *Online Piracy in Numbers*, 2011, Go-Gulf, http://www.go-gulf.com/blog/online- piracy/(last viewed Dec.17, 2014).

9 Gabe Friedman, *The Biggest Filer of Copyright Lawsuits? This Erotica Website*, The New Yorker, http://www.newyorker.com/business/currency/the-biggest- filer-of-copyright-lawsuits-this-erotica-web-site (last viewed Dec. 17, 2014).

10 Julianne Pepitone, *50,000 BitTorrent users sued for alleged illegal downloads*, CNN Money, http://money.cnn.com/2011/06/10/technology/bittorrent\_lawsuits /index.htm (last viewed Dec.17, 2014).

11 *Elf-Man, Inc. v. Does 1-36*, 2013 U.S. Dist. LEXIS 66319; Kelly/Warner Law, http://kellywarnerlaw.com/elf-man-illegal-downloading-lawsuits/

(last viewed Dec. 17, 2014)

12 *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80 (2012), \*83, \*85

13 *Third Degree Films, Inc. v. Doe*, 2013 U.S. Dist. LEXIS 44131, \*5,\*7

14 *Elf-Man, Inc. v. Does 1-36*, 2013 U.S. Dist. LEXIS 66319, \*4

15 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 548 (2007).

16 *Fleurimond v. N.Y. Univ*., 722 F. Supp. 2d 352, 354 (2010).

17 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 560 (2007).

18 *Id. at* 562.

19 *Ashcroft v. Iqbal*, 556 U.S. 662, 673 (2009).

20 *Patrick Collins v. Doe 1*, 945 F. Supp. 2d 367, 373-74 (2013).

21 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

22 *Id.* at 552.

23 *Id*. at 557.

24 *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009).

25*Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

26 *Id*. at 557.

27 *Id*. at 559.

28 *Id*. at 558.

29 *Patrick Collins, Inc. v. Doe 1*, 945 F.Supp. 2d 367, 369 (2013)

30 *Id*. at 371.

31 *Id*. at 374.

32 *Id*. at 375.

33 *John Wiley & Sons, Inc. v. Doe Nos. 1-30*, 2012 U.S. Dist. LEXIS 182741, \*6

34 *Braun v. Primary Distributor Doe,* 2012 U.S. Dist. LEXIS 173465, \*6

35 *Elf-Man, Inc. v. Does 1-36*, 2013 U.S. Dist. LEXIS 66319, \*5

36 *Id*. at \*6.

37 *Patrick Collins, Inc. v. Doe 1*, 945 F.Supp. 2d 367, 372 (2013).

38 *Id*. at 374.

39 *Id*. at 371.

40 *Id*. at 375.

41 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007).

42 *Patrick Collins, Inc. v. Doe 1*, 945 F.Supp. 2d 367, 372 (2013).

43 Vago, Steven. *Law and Society*. Sixth ed. Englewood Cliffs, NJ: Prentice-Hall, 1981. Print. P.3.

44 The Bridge, http://cyber.law.harvard.edu/bridge/LawSociety/essay1.htm

(last viewed Dec.19, 2014).

45 Vago, Steven. *Law and Society*. Sixth ed. Englewood Cliffs, NJ: Prentice-Hall, 1981. Print. P.19.

46 *Id*. at 2.

47 *Id*. at 174.

48 *Id*. at 177-78.

49 *Id*. at 178.

50 *Id*. at 17.

51 *Id*. at 18.

52 *Id*. at 212.

53 *Id*. at 18.

54 *Id*. at 17.

55 *Id*. at 212.

56 *Id.* at 216.

57 W*hat can a hacker do with an IP address?*, Information Security, stack exchange inc., http://security.stackexchange.com/questions/19018/what-can-a-hacker- do-with-an-ip-address (last visited Dec.19, 2014).

58 *Cruz v. Middlekauf Lincoln-Mercury*, 909 P.2d 1252, 1253 (1996).

59 U.S. Dept. of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/ understanding/consumers/noticepp.html (last viewed Dec. 19, 2014).

60 *First Time Videos, LLC v. Doe*, 276 F.R.D. 241,247 (2011).

61 *Id*. at 248.

62 *Id*. at 249.

63 *Id*. at 250.

64 *Voltage Pictures, LLC v. Doe*, 818 F. Supp. 2d 28, 35 (2011).

65 *Id.* at 36*; First Time Videos, LLC v. Doe*, 276 F.R.D. 241,248 (2011); *John Wiley & Sons, Inc. v. John Does Nos.* *1-35*, 2012 U.S. Dist. LEXIS 182741, \*4-5

66 *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80 (2012), \*82; Ernesto, *Judge: IP-Address is Not a Person and Can't Identify a BitTorrent Pirate*, https://torrentfreak.com/ip-address-not-person-140324/ (last viewed Dec.20, 2014).

67 *Id*.

68 *Malibu Media, LLC v. Doe*, 2014 U.S. Dist. LEXIS 82480, \*5

69 *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.RD. 80,84 (2012).

70 *Id*. at 85.

71 *Elf-Man, LLC v. Doe*, 2013 U.S. Dist. LEXIS 112128, \*10

72 Ernesto, *Judge: IP-Address Does Not Prove Copyright Infringement, https://torrentfreak.com/judge-ip-address-does-not-prove-copyright- infringement-140121/*(last viewed Dec. 20, 2014).

73 Boldrin, Michele, and David K. Levine. *Against Intellectual Monopoly*. New York: Cambridge UP, 2008. Print. P.17.

74 *Id*. at 109.

75 *Id*. at 17.

76 *Id*. at 53.

77 *Id*. at 35.

78 *Id*. at 37.

79 *Id*. at 54.

80 *Id*. at 34.

81 *Id*. at 19.

82 *Id*. at 135.

83 *Id*. at 114.

84 *Id*. at 120.