# Washington Journal of Law, Technology & Arts

*University of Washington School of Law*

VOL. 7 WINTER 2012 NO. 3

CONTENTS

# Washington Journal of Law, Technology & Arts

*University of Washington School of Law*

VOL. 7 WINTER 2012 NO. 3

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 3 WINTER 2012

# UNDERSTANDING AND AUTHENTICATING EVIDENCE FROM SOCIAL NETWORKING SITES

*Heather L. Griffith*[*]


CITE AS: 7 WASH J.L. TECH. & ARTS 209 (2012)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1111

## ABSTRACT

*Social networking is a popular form of online interaction that combines several types of electronic communication in a single user interface. An attorney working with evidence found on social networking sites should have a general understanding of how users create and access content on social networking platforms. Before such evidence may be presented to the jury, an attorney must make a showing of authenticity. The proponent of the evidence may need to use different authentication methods depending on the type of communication involved. This Article provides background information about social networks and explores how to authenticate common types of evidence available on social networking sites.*

[*] Heather L. Griffith, University of Washington School of Law, Class of 2012. Thank you to Professor Anita Krug and Articles Editor Jeff Doty for their comments and insights.

TABLE OF CONTENTS



## INTRODUCTION

Social networking sites are rapidly becoming a standard method of communication for millions of users. Attorneys may find evidence of these communications useful during trial. Attorneys have sought to introduce evidence from social networking sites, including photographs to show gang affiliation,[1] posts to show witness intimidation,[2] and messages as evidence against a defendant accused of domestic violence.[3] Authentication, a prerequisite to the admission of evidence at trial, requires a showing that the evidence in question is what its proponent claims.[4]

Social networking sites present unique challenges for authentication. These sites are different than other types of electronic evidence because users create individual profile pages. Most users post identifying information on profile pages; however, social networks are pseudonymous—postings are linked to the person who

---

[1] People v. Lenihan, 911 N.Y.S.2d 588, 592 (N.Y. Sup. Ct. 2010).

[2] Griffin v. State, 19 A.3d 415, 418 (Md. 2011).

[3] People v. Goins, No. 289039, 2010 WL 199602, at *2 (Mich. Ct. App. Jan. 21, 2010).

[4] FED. R. EVID. 901(a).

posted them only through the information he or she has chosen to put on the profile. In addition, questions of who accessed and used the social networking site may arise at trial.[5] Often, the proponent must show that a particular person authored the communication, and not simply that it came from a specific social networking profile.[6]

As social networking sites become more prevalent, litigators must understand how to authenticate the various electronic formats presented by sites such as MySpace and Facebook. Evidence from these sites may take the form of profile pages, postings, chats, private messages, photos, or video. Authenticating evidence from these social networking sites may involve different methods, depending on the type of communication. Given the time and expense involved, the litigator must know how much foundational evidence a court will require for authentication.

Courts may authenticate evidence from social networking sites by use of distinctive characteristics, testimony of a witness with knowledge, or process testimony, such as testimony from a computer expert. Although users of these sites often fill their profile pages with individualized and distinctive content, the trend in the courts is to require more evidence than just a particularized profile page to authenticate a specific posting on the site. If the characteristics of the specific communication in question are genuinely distinctive, courts will allow circumstantial authentication based on content and context.[7] However, courts will require additional corroborating evidence if the characteristics are more general.[8]

This Article begins with a guide to understanding how users interact via social networking sites and description of the various forms of evidence on social networking sites. Next, the Article applies the standard for authenticating evidence to social networking sites. The discussion continues with methods of authentication for categories of evidence from social networking sites, including profiles and posts, e-mails and chats, and photographs and video.

---

[5] *See, e.g.*, Tienda v. State, No. PD–0312–11, 2012 WL 385381, at *3 (Tex. Crim. App. Feb. 8, 2012).

[6] *See, e.g.*, State v. Eleck, 23 A.3d 818, 824 (Conn. App. Ct. 2011).

[7] *See, e.g.*, *Tienda*, 2012 WL 385381, at *7.

[8] *See, e.g.*, Griffin v. State, 19 A.3d 415, 424 (Md. 2011).

## I. A GUIDE TO SOCIAL NETWORKING SITES

Social networking sites are quickly becoming a common form of communication. MySpace and Facebook are among the most popular sites, and many other sites operate in a similar manner. This section discusses the basic setup for Facebook and MySpace and the ways users interact through these sites.[9] On traditional websites, the site's owner typically creates content and makes it available on the Web for others to view. On social networking sites, individual users create content inside a framework provided by the site's owner.

A user logs in to an account much like logging in to an e-mail account. Each user has a unique username and password that the user selects when setting up the account.[10] Most social networking sites do not verify the identity of the person creating the account.

A unique feature of social networking sites is the individual profile page.[11] This profile page is a Web page that the user maintains. Typically, profiles contain personal details, such as the user's name, birthday, gender, current city, interests, or other identifying information.[12] A picture, commonly called a "profile picture," is usually attached to the profile. Sometimes users choose to use the social network pseudonymously and do not provide accurate information or their real name on the profile.[13]

After an individual creates a profile page, she establishes connections with other people on the social network. Users connect to one another by linking their profiles to others' profile through a

---

[9] MySpace and Facebook are general-purpose social networking sites. Some sites have specific purposes: for example, LinkedIn is designed for professional networking. For a description of some of the different kinds of social networking sites not covered by this article, *see A Trial Lawyer's Guide to Social Networking Sites*, DELIBERATIONS: LAW, NEWS, AND THOUGHTS ON LITIGATION CONSULTING BY THE AMERICAN SOCIETY OF TRIAL CONSULTANTS (ASTC), http://jurylaw.typepad.com/deliberations/social_networking.html (last visited Jan. 9, 2011).

[10] *See Login Basics - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/login/basics (last visited Nov. 28, 2011).

[11] *See Griffin*, 19 A.3d at 426 n.13.

[12] *Griffin*, 19 A.3d at 420; *Editing My Profile Information - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/?page=216501321702579 (last visited Nov. 28, 2011).

[13] *Griffin*, 19 A.3d at 421.

process commonly referred to as "friending."[14] The virtual friendship is usually established by one user requesting to link to another user's page via a "friend request" and the second user confirming the friendship request.[15] Once the friendship is confirmed, a link appears on the profile page of both individuals. Some users only friend people they have met in person, while others will friend people they have met only through the online network. By establishing friendships, an individual creates a network of users with whom to interact.

There are many ways to interact with other individuals on a social networking site, including "posting" and "tagging." When "posting," users add information, links, pictures, or videos for others to see.[16] For example, John may post a link to an interesting online article, and Mary might comment on the post with her opinion of the article. Mary's comments are linked to her profile by her "profile picture" and the name on her profile page. Another type of interaction occurs when users upload content such as digital photographs, audio files, and video onto the site and then "tag" other users.[17] For example, a person might upload a photograph and then tag a sibling who also appears in the photograph. The tag creates a link from the photograph to the profile page of the sibling. Instead of being sent privately to an intended recipient, posts, and tags pages are published either publicly or to a group of "friends," depending on the user's privacy settings.[18] These interactions are recorded on the profile page, creating content on the site, and are available for others to view. A person may log in to the site to view the new content that has been created by those in her "friend" network.

Users also may interact directly with each other by sending private, e-mail-like messages or by chatting (also called instant

---

[14] *Adding Friends & Friend Requests - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/friends/requests (last visited Nov. 28, 2011).

[15] *Griffin*, 19 A.3d at 420.

[16] *How to Post and Share - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/?page=125122004234100 (last visited Nov. 28, 2011).

[17] *Tagging - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/tagging (last visited Nov. 28, 2011).

[18] *Griffin*, 19 A.3d at 420, 426 n.13; *News Feed basics - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/?page=132070650202524 (last visited Nov. 28, 2011).

messaging).[19] This third type of interaction does not create content on the profile page, but the individual receiving the e-mail or chat can connect to the profile page of the sender. Depending on a user's privacy settings, the site may retain a transcript of the chat session.

To control who may view profile page content, social networking sites have a variety of privacy settings.[20] Some users choose to make all or most of their content "public." This means that it is available on the Internet for anyone to see, even those who do not have an account with the social networking site. Some users make content more private by only allowing the people they have accepted as "friends" to see their information.[21] Users also may allow only specific friends to see certain content.

## II. THE FEDERAL STANDARD FOR AUTHENTICATION OF EVIDENCE FROM SOCIAL NETWORKING SITES

An attorney seeking to introduce evidence from social networking sites must overcome the hurdle of authentication.[22] The proponent must provide foundational evidence to show that the evidence in question is what the proponent claims.[23] Authentication of evidence involves a two-step process. First, the court makes a preliminary determination of authenticity.[24] Rule 901(a) of the Federal Rules of Evidence[25] lays out the standard for the court's preliminary

---

[19] *Messages basics - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/messages/basics (last visited Nov. 28, 2011); *Basics: How to Chat - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/chat/basics (last visited Nov. 28, 2011).

[20] For a discussion on the difficulties of managing privacy on social networking sites, *see* JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 54-59 (2008).

[21] *See, e.g.*, A.B. v. State, 885 N.E.2d 1223, 1227 (Ind. 2008) (distinguishing posts made on a "private" MySpace profile from those made on a publically accessible profile); *Basic Privacy Controls - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/privacy/basic-controls (last visited Nov. 28, 2011).

[22] *See generally*, 5 JACK B. WEINSTEIN & MARGARET A. B`ERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.06 (2011). There may be other barriers to admissibility, such as the rule against hearsay. *Id.* at § 900.06[1][c][ii].

[23] FED. R. EVID. 901(a).

[24] *Id.*

[25] This section considers the standard under the Federal Rules of Evidence, but

determination, requiring "evidence [of authenticity] sufficient to support a finding that the matter in question is what its proponent claims."[26] The standard is low: the evidence of authenticity must be enough to provide a rational basis for a jury to find that it is authentic.[27] The evidence need not be conclusive and it may be circumstantial.[28] Second, after the court has made a preliminary finding that the evidence is what the proponent claims, the evidence is introduced and subject to cross examination. The jury considers the evidence and makes the ultimate determination of authenticity, weighing the evidence accordingly.[29]

Evidence from social networking sites may present challenges for authentication, but the traditional rules still apply. Rather than creating a new body of law, courts have adapted traditional methods of authentication to accommodate electronic evidence, including evidence from social networking sites.[30] Consequently, courts determine authenticity of electronic evidence "on a case-by-case basis as any other document."[31]

Rule 901(b) illustrates several ways to authenticate evidence, including "Testimony of witness with knowledge"; "Distinctive characteristics and the like"; and "Process or system."[32] An attorney may combine these approaches to authenticate a particular piece of evidence.

First, a witness may testify that the evidence is what it purports to

---

many state rules are substantially similar.

[26] FED. R. EVID. 901(a). The courts treat this as a question of conditional relevance under Rule 104(b). WEINSTEIN & BERGER, *supra* note 22, § 900.06[1][c][i].

[27] State v. Bell, No. CA2008-05-044, 2009 WL 1395857, at *3 (Ohio Ct. App. May 18, 2009), *appeal denied*, 914 N.E.2d 1064 (Ohio 2009).

[28] *Id.*; Manuel v. State, No. 12–09–00454–CR, 2011 WL 3837561, at *6 (Tex. App. Aug. 31, 2011).

[29] 4 DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW, § 5.03[1], at 5-57 (rev. ed. 2010).

[30] *See, e.g.*, State v. Eleck, 23 A.3d 818, 823 (Conn. App. Ct. 2011); *see also* PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 339 (Am. Bar Ass'n, 2d ed. 2008). The rules were meant to "[l]eave room for growth and development." FED. R. EVID. 901, advisory comm. note.

[31] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543 (D. Md. 2007) (quoting In Re F.P., 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005)).

[32] FED. R. EVID. 901(b).

be. For example, a witness may testify that he or she created the social network profile and posted the communication.[33]

Second, "[t]he characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety."[34] Courts have noted that the type of circumstantial evidence used for authentication changes with the medium of communication.[35] This method of authentication is particularly useful for evidence from social networking sites, where users often post identifying information.

Third, process or system authentication requires evidence "showing that the process or system produces an accurate result."[36] In cases involving evidence from social networking sites, a non-expert computer user provides authenticating testimony by testifying as to how she logged into the account and viewed the social network profile at issue, and that the printed copies are a true and correct representation of what she viewed.[37] Testimony by a computer expert or administrator of the social networking site may also assist in authentication,[38] such as when an expert determines that a particular computer was used to create the profile or a specific posting.[39]

In addition, if the foundation for authentication of evidence is weak, the probative value is limited. The court may exclude the evidence because "its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury."[40]

Once the court makes a preliminary determination of authenticity, the evidence is presented to the jury. The jury decides how to weigh any further concerns about the veracity of the evidence, such as those

---

[33] Griffin v. State, 19 A.3d 415, 427 (Md. 2011).

[34] FED. R. EVID. 901, advisory comm. note; *see also Lorraine*, 241 F.R.D. at 546.

[35] *Eleck*, 23 A.3d at 823.

[36] FED. R. EVID. 901(b)(9).

[37] *See, e.g.*, Dockery v. Dockery, E2009-01059-COA-R3-CV, 2009 WL 3486662, at *6 (Tenn. Ct. App. Oct. 29, 2009).

[38] *See, e.g.*, People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009), *appeal denied*, 925 N.E.2d 937 (2010); Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010).

[39] Griffin v. State, 19 A.3d 415, 427 (Md. 2011).

[40] FED. R. EVID. 403; WEINSTEIN & BERGER, *supra* note 22, § 900.06[2][b].

raised on cross-examination. This weighing goes to the credibility of the evidence, which is within the province of the jury, not the judge. For example, one court specified that the possibility that someone else accessed the defendant's social networking account was a question appropriately left for the jury.[41]

There are two distinct types of authentication that must occur for evidence from social networking sites. One is to authenticate the authorship of the evidence on the website, which is the focus of this Article. The other is to authenticate that the exhibit used at trial, typically a printout of the webpage, is a fair and accurate representation of what was on the computer screen. Testimony by a witness who viewed the information on the website is usually sufficient to meet the latter requirement.[42]

## III. AUTHENTICATION OF PROFILES AND POSTINGS

Social networking sites differ from other types of electronic evidence because users create an individual profile page. Users often fill their profile pages with individualized and distinctive content. However, the trend in the courts is to require more evidence than just a distinctive profile page to authenticate a specific posting on the site. Often, the proponent must show that a specific person authored the writing, and not just that the writing came from that person's account. This evidence could take the form of distinctive characteristics within the specific posting itself; testimony from a witness with knowledge of the posting; process testimony, such as forensic computer evidence; or a combination of these methods.

A profile on a social networking site generally contains unique content connecting it to the person who created the page, even if the user posts under a false name. One Texas appellate court stated:

> The inherent nature of social networking websites encourages members who choose to use pseudonyms to identify themselves by posting profile pictures or descriptions of their physical appearances, personal backgrounds, and lifestyles. This type of

---

[41] *Clevenstine*, 891 N.Y.S.2d at 514.

[42] WEINSTEIN & BERGER, *supra* note 22, § 900.07[5].

> individualization is significant in authenticating a particular profile page as having been created by the person depicted in it.[43]

The court further stated that the more particular and distinctive the information is, the more likely a court will find it authentic.[44]

However, a personalized profile, by itself, is not usually enough to authenticate evidence from social networking sites.[45] The fact that a witness held and managed an account does not provide enough of a foundation for authentication; the proponent must show that the communication in question came from the witness and "not simply from her Facebook account."[46] Courts have raised concerns because social networking accounts may be compromised by hackers[47] and anyone may create a fictitious account under another's name.[48] In addition, users "frequently remain logged in to their accounts while leaving their computers and cell phones unattended,"[49] raising the likelihood of third parties creating unauthorized posts. The proponent of the evidence should address these concerns when laying the foundation for authentication.

### *A. Authentication by Distinctive Characteristics*

A court may find a profile page authentic if the content of the page or the posting is so distinctive that it only could have been created by one particular individual. Concerns of misuse of the social networking account are alleviated because the substance of the communication is so distinctive. A Michigan case, *People v. Goins*, demonstrates how evidence from social networking sites may be

---

[43] Tienda v. State, No. 05–09–00553–CR, 2010 WL 5129722, at *5 (Tex. App. Dec. 17, 2010), *aff'd*, No. PD–0312–11, 2012 WL 385381 (Tex. Crim. App. Feb. 8, 2012).

[44] *Id.*

[45] *See, e.g.*, Griffin v. State, 19 A.3d 415 (Md. 2011); People v. Padilla, No. F056829, 2010 WL 4299091, at *19-20 (Cal. Ct. App. Nov. 1, 2010); State v. Eleck, 23 A.3d 818, 824 (Conn. App. Ct. 2011).

[46] *Eleck*, 23 A.3d at 824 (Conn. App. Ct. 2011).

[47] *Id.* at 822.

[48] *Griffin*, 19 A.3d at 421.

[49] *Eleck*, 23 A.3d at 822.

authenticated by distinctive content and context.[50] The Michigan Court of Appeals stated that "what certainly appears to be Bradley's [the victim] MySpace page" contains "descriptive details of the assault that fit within what a reasonable person would consider to be 'distinctive content' not generally known to anyone other than Bradley, defendant, or someone in whom one or the other confided."[51] The court held that these indicia were sufficient for the jury to reasonably find that Bradley was the author of the MySpace content.[52]

Similarly, in *Tienda v. State*, Texas' highest criminal court authenticated a MySpace page not only because it contained the defendant's name, nicknames, city, and numerous photographs; but because it also contained references to the crime, arrest, and subsequent electronic monitoring.[53] The court found "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them."[54] The distinctive characteristics allowed the jury to infer that it was unlikely that anyone else created the social networking profile or post.

Courts have not authenticated evidence from profile pages or posts when they contain only general information about a witness.[55] In *Griffin v. State*, Maryland's highest court held that a witness's birthday, location, photograph, and use of a nickname did not provide a foundation to authenticate the profile.[56] Information that is generally known by a witness's associates and friends is not "distinctive" and thus cannot be enough to authenticate a profile page. In this situation, the proponent may provide additional evidence

---

[50] People v. Goins, No. 289039, 2010 WL 199602, at *2 (Mich. Ct. App. Jan. 21, 2010).

[51] *Id.*

[52] *Id.*

[53] Tienda v. State, No. PD–0312–11, 2012 WL 385381, at *7 (Tex. Crim. App. Feb. 8, 2012).

[54] *Id.*

[55] *See, e.g.*, Griffin v. State, 19 A.3d 415 (Md. 2011); State v. Eleck, 23 A.3d 818, 824 (Conn. App. Ct. 2011); People v. Padilla, No. F056829, 2010 WL 4299091, at *17-18 (Cal. Ct. App. Nov. 1, 2010).

[56] *Griffin*, 19 A.3d at 424.

for authentication.

### *B. Corroborating Non-Distinctive Characteristics on Profile Pages or Posts with Additional Evidence*

Authentication of evidence from social networking sites may require the attorney to use multiple methods of authentication. In some situations, the individualized characteristics of the profile page are not distinctive enough to allow for authentication. The proponent should introduce corroborating evidence to provide further foundation for authentication. In addition, the proponent should use process testimony to demonstrate that the printed court exhibits are true and correct representations of the Web page.

Corroborating evidence may take the form of testimony of a witness with knowledge or process testimony by a computer expert. A witness can testify that she authored a particular post, or that she saw someone author it.[57] Courts have also sought evidence relating to "who had access to the [Web] page and whether another author . . . could have virtually-penned the messages."[58] Expert computer testimony will also assist in authentication, such as by determining whether a particular computer was used to create the posting or profile in question.[59] Expert testimony can provide the court information "regarding how secure such a Web page is, who can access a My[S]pace Web page, whether codes are needed for such access, etc."[60]

Mere testimony from a person viewing a MySpace page is not sufficient to establish that the content is from a particular party.[61] The Massachusetts Supreme Court likened the electronic communication to a telephone call, saying: "a witness's testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, is insufficient evidence to admit the call as a conversation with 'A.'"[62]

---

[57] *See id.* at 427.
[58] *Id.* at 425; *see also Padilla*, 2010 WL 4299091, at *19.
[59] *Id.* at 427.
[60] Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010).
[61] *Williams*, 926 N.E.2d at 1171; *see Griffin*, 19 A.3d at 418.
[62] *Id.*

## IV. AUTHENTICATION OF E-MAIL AND CHATS FROM SOCIAL NETWORKING SITES

Other types of evidence from social networking sites are analogous to more familiar forms of electronic evidence. While jurisdictional rules may vary, courts generally have established methods for authentication of e-mail and Internet chat.[63]

Courts have compared messages sent privately between profiles on social networking sites to e-mail and traditional letters.[64] Standard e-mail messages are often authenticated either by someone with personal knowledge of the transmission (or receipt) or circumstantially through the use of distinctive characteristics.[65] Private messages sent through social networking sites may also be authenticated in the same way. For example, a California court permitted authentication based on testimony from the victim that he sent messages and received replies, and "based on their content, he believed he was communicating with the defendant."[66] When the defendant challenged the authenticity of the printouts of the messages, the court said that any possibility that the messages were written by someone else went to the weight of the evidence and left the final determination of authenticity to the jury.[67]

Chatting using social networking sites is similar to Internet chatting using other websites. Courts have permitted authentication of Internet chats by the use distinctive characteristics.[68] Chat conversations using social networking sites are linked to an individual profile page. In *State v. Bell*, an Ohio case, the information on a MySpace profile served to corroborate the distinctive characteristics contained within chat messages.[69] A witness had MySpace e-mails and online conversations with the defendant. The

---

[63] For a more detailed discussion of e-mail and chat authentication, *see generally* WEINSTEIN & BERGER, *supra* note 22, §§ 901.08[3]-[4].

[64] *See* People v. Fielding, No. C062022, 2010 WL 2473344, at *4 (Cal. Ct. App. June 18, 2010), review denied (Sept. 1, 2010).

[65] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 554-55 (D. Md. 2007).

[66] *Fielding*, 2010 WL 2473344, at *5.

[67] *Id.* at *3-5.

[68] *Lorraine*, 241 F.R.D. at 556.

[69] State v. Bell, 882 N.E.2d 502, 511 (Ohio Ct. Com. Pl. 2009), *aff'd*, No. CA 2008-05-044, 2009 WL 1395857 (Ohio Ct. App. May 18, 2009).

witness, T.W., testified that he accessed the messages by logging into his MySpace profile and that the printouts were accurate records of his conversation.[70] T.W.'s testimony was sufficient for authentication because of his knowledge of the defendant's MySpace username and the code words contained in the communications that would only be known by the defendant and T.W.[71]

In cases where communications do not contain distinctive characteristics, courts may require expert testimony or other corroborating evidence for authentication. For example, the Massachusetts Supreme Court in *Commonwealth v. Williams* held that the proponent of evidence from a MySpace account had only shown the evidence came from a particular profile page, and not from a specific person.[72] The trial court should not have admitted the evidence without additional foundational testimony.[73]

## V. AUTHENTICATION OF PHOTOGRAPHS AND VIDEO FROM SOCIAL NETWORKING SITES

An individual may post digital photographs or videos on social networking sites, but they cannot be authenticated by distinctive characteristics alone. While a photograph is linked to the profile page of the person who posted it, there is nothing connecting the person who posted the photo to the place and time where the photograph was taken.[74] For example, a person may take an image from an unrelated website, copy it, and then post it on a MySpace profile. Thus, photographs from social networking sites may not be authenticated by the distinctive characteristics of a profile page.[75]

---

[70] State v. Bell, No. CA 2008-05-044, 2009 WL 1395857, at *5 (Ohio Ct. App. May 18, 2009).

[71] State v. Bell, 882 N.E.2d 502, 512 (Ohio Ct. Com. Pl. 2009), *aff'd*, No. CA 2008-05-044, 2009 WL 1395857 (Ohio Ct. App. May 18, 2009).

[72] Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010).

[73] *Id.*

[74] *See* People v. Ulloa, No. B223203, 2011 WL 3131022, at *6 (Cal. Ct. App. June 22, 2011); People v. Hernandez, No. B216495, 2010 WL 4983290, at *7-8 (Cal. Ct. App. Dec. 9, 2010).

[75] *See, e.g.*, People v. Beckley, 110 Cal. Rptr. 3d 362, 366 (Cal. Ct. App. 2010), *cert. denied*, 131 S.Ct. 1522 (2011); People v. Lenihan, 911 N.Y.S.2d 588, 592 (N.Y. Sup. Ct. 2010).

The two typical ways to authenticate a digital photograph, regardless of the source of the photograph, are (1) testimony from someone present at the time the photograph was taken or (2) expert testimony that the photograph was not altered.[76] Digital videos have similar standards for authentication.[77] Proponents of evidence from social networking sites should also use these standards.

## CONCLUSION

Social networking websites may contain several types of electronic evidence, including profile pages, posts, private e-mail messages, chats, photographs, and video. Profiles pages, posts, messages, and chats sometimes contain distinctive characteristics that allow for authentication. This evidence must be in the specific communication at issue and distinctive enough to show who authored the communication. If the evidence does not contain distinctive characteristics, the court will require additional foundational evidence for authentication, such as testimony of a witness with knowledge or testimony from a computer expert. Proper foundational evidence will help the proponent of the evidence properly authenticate evidence from social networking sites.

## PRACTICE POINTERS

- Attorneys need to understand the type of electronic evidence they are authenticating. Evidence from social networking sites may include profile pages, chat transcripts, public messages, private e-mail-type messages, digital photographs, or video.
- Users of social networks often post identifying information. If this information contains unique and distinctive characteristics, it may be used to aid authentication.
- If the information posted on the social networking site is generally known in the user's community, it is not sufficient for authentication and additional foundational evidence is

---

[76] *Beckley*, 110 Cal. Rptr. 3d at 366-67, *see also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561-62 (D. Md. 2007).

[77] *See* WEINSTEIN & BERGER, *supra* note 22, § 901.05[1].

required. This may take the form of testimony of a person with knowledge of who posted the information, a computer expert, or a person from the company that runs the social networking site.

- The person who accessed the social networking site should testify as to how the page was accessed. This witness should also verify that the printouts used in court are a true and accurate copy of what the witness saw on the computer screen.
- Photographs and video taken from social networking sites cannot be authenticated by distinctive characteristics of a profile page. The standard methods for authentication of photographs and video still apply.
- The possibility that another party accessed and used an account usually goes to the weight of the evidence, not admissibility.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 3 WINTER 2012

# LET'S BE CAUTIOUS FRIENDS: THE ETHICAL IMPLICATIONS OF SOCIAL NETWORKING FOR MEMBERS OF THE JUDICIARY

*Aurora J. Wilson*[*]


Cite as: 7 Wash J.L. Tech. & Arts 225 (2012)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1112

ABSTRACT

*In recent advisory opinions, courts and ethics committees have considered whether and to what extent judges may use social networking sites such as Facebook without violating the applicable code of judicial conduct. While the committees agree that judges may generally use social networking sites, they disagree as to whether judges may use those sites to connect with lawyers who have appeared or may appear in a proceeding before them. Four states—California, Florida, Massachusetts, and Oklahoma—forbid judges from becoming online "friends" with attorneys who may appear before them in court, while four states—Ohio, Kentucky, New York, and South Carolina—allow it, albeit with caution. This Article examines the recent trend in advisory opinions governing the use of social media by members of the judiciary and provides practical advice for judges to conform to the code of judicial conduct.*

[*] Aurora J. Wilson, University of Washington School of Law, Class of 2012. Thank you to Professor Anita Ramasastry and Associate Editor-in-Chief Heather Griffith.

TABLE OF CONTENTS



## INTRODUCTION

As the use of social media rises, a number of state ethics committees have begun to analyze the ethical ramifications for judges who participate in online social networking. Recent advisory opinions generally opine that judges may use social networking sites such as Facebook without violating governing ethical canons. However, these opinions also recognize that in certain circumstances a judge's use of social networking may run afoul of the ethical duties imposed by the state's code of judicial conduct. This Article explores the ethical duties applicable to judges who use social networking sites, as well as the prospective ramifications of judges' social networking activities. Finally, the Article provides guidelines for judges to conform to acceptable, ethical conduct on social media sites.

## I. OVERVIEW OF SOCIAL NETWORKING AND ITS PREVALENCE AMONG MEMBERS OF THE LEGAL PROFESSION

Social networking involves the use of interactive websites and

programs that allow people to share "information, knowledge and experiences" by connecting with and forming communities among other users.[1] Popular social networking sites include Facebook, MySpace, Twitter, and LinkedIn, among others. These sites use terms such as "friends" (on Facebook) and "connections" (on LinkedIn) to signal a networking relationship between users.[2] In order to "friend" or "connect with" another user on the network, an individual must submit a request to that user. Once the other user accepts, the users become "friends" and may interact online.

The nature and level of online interactions between "friends" or "connections" varies by type of social networking site and by the privacy settings each user selects. On Facebook, "friends" may often see one another's profile pages, pictures, comments, and status updates. Facebook friends usually interact by posting comments on friends' profile sites or posts, sending messages, chatting online, "liking" one another's posts and pictures, and sharing or commenting on status updates and photographs.[3] Unless a user selects enhanced privacy settings, other friends in the same network may also view these interactions.[4] Google+ and MySpace function in much the same way as Facebook, while LinkedIn deemphasizes personal status posts and pictures in favor of sharing information related to work experience and professional development.

Social networking sites have skyrocketed in popularity since their inception circa 2003. Facebook currently boasts more than 845 million active users,[5] Google+ claims to have 150 million users,[6]

---

[1] *New Media and the Courts: The Current Status and a Look at the Future*, NEW MEDIA COMM. OF THE CONFERENCE OF COURT PUBLIC INFO. OFFICERS 19 (Aug. 26, 2010), *available at* http://www.ccpio.org/documents/newmediaproject/New-Media-and-the-Courts-Report.pdf.

[2] *Id.* at 28.

[3] SUPREME COURT OF OHIO BOARD OF COMM. ON GRIEVANCES AND DISCIPLINE, OP. 2010-7 (2010), *available at* http://www.supremecourt.ohio.gov/Boards/BOC/Advisory_Opinions/2010/default.asp [hereinafter OHIO OP. 2010-7].

[4] *Id.*

[5] *Facebook's latest news, announcements and media resources - Fact Sheet*, FACEBOOK, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (last visited Feb. 12, 2012).

[6] *Google+ Has Reached 150 million active users according to un-official statistics, really?*, GOOGLE+ NEWS, (Dec. 25, 2011), http://google-plus.com/3924/google-has-reached-150-million-active-users-according-to-un-

LinkedIn connects some 135 million professionals,[7] and MySpace hosts approximately 150 million subscribers.[8] Social networking sites are popular not only among the general public, but also among members of the legal profession. One recent study investigated the use of social media by the judiciary and found that nearly 40 percent of the judges surveyed used a social networking site—predominantly Facebook—while approximately seven percent of courts surveyed had business profiles on social media sites such as Facebook or Twitter.[9]

## II. THE ETHICAL IMPLICATIONS OF SOCIAL NETWORKING

The prevalence of social networking by members of the legal profession highlights the need for clear ethical standards governing online behavior. Judges are central and public figures in the U.S. legal system and are therefore held to high ethical standards in all aspects of their professional and personal lives.[10] Indeed, the American Bar Association (ABA) Model Code of Judicial Conduct prescribes that judges are bound to represent and uphold the honor and integrity of the legal system in all activities, whether judicial or extra-judicial.[11] Given the semi-public nature of social networking "friendships" and the associated risk of public scrutiny, participation in social networking sites may be especially problematic for judges.

As several state ethics committees have recently noted, a judge's use of social networking sites implicates various canons of the Code of Judicial Conduct. Specifically, certain canons require a judge to

---

official-statistics-really/.

[7] *About Us*, LINKEDIN, http://press.linkedin.com/about (last visited Feb. 12, 2012).

[8] *MySpace Usage Statistics*, BUILTWITH TECHNOLOGY USAGE STATISTICS, http://trends.builtwith.com/cms/MySpace (last visited Feb. 12, 2012).

[9] *New Media and the Courts: The Current Status and a Look at the Future*, NEW MEDIA COMM. OF THE CONFERENCE OF COURT PUBLIC INFO. OFFICERS, 65 (Aug. 26, 2010), *available at* http://www.ccpio.org/documents/newmediaproject/New-Media-and-the-Courts-Report.pdf.

[10] AMERICAN BAR ASSOCIATION, MODEL CODE OF JUDICIAL CONDUCT, Preamble, (2010), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_code_of_judicial_conduct.

[11] *Id.*

avoid conduct that would give the appearance of impropriety or outside influence, and to abstain from conduct that could create a conflict of interest or the appearance of such a conflict.[12] As the advisory opinions demonstrate, a judge is more likely to violate these ethical duties by accepting a "friend request" from a party who will appear or has appeared before the judge in court. Given the concern over the potential impropriety of such online "friendships" and the subsequent communications involved, ethics committees in at least seven states to date have considered the ethical ramifications for judges who partake in online social networking.

## III. MOST ADVISORY COMMITTEES AGREE: JUDGES MAY USE SOCIAL NETWORKING SITES

While many states have yet to consider the ethical duties imposed on attorneys or judges involved in social networking, the emerging consensus holds that the ethical standards set forth in the Code of Judicial Conduct do not prohibit a judge from using social networking sites. State ethics committees in California, Kentucky, Massachusetts, Ohio, Oklahoma, New York, South Carolina, and Florida agree that a judge may use social networking sites, provided the use adheres to certain limitations.[13] Some states, including Ohio

---

[12] *See id. at* Canon 2; Canon 3.

[13] *See* OHIO OP. 2010-7; S.C. ADVISORY COMM. ON STANDARDS OF JUDICIAL CONDUCT, OP. 17-2009 (2009), *available at* http://www.judicial.state.sc.us/advisoryOpinions/displayadvopin.cfm?advOpinNo=17-2009 [hereinafter S.C. OP. 17-2009]; N.Y. ADVISORY COMM. ON JUDICIAL ETHICS, OP. 08-176 (2009), *available at* www.nycourts.gov/ip/judicialethics/opinions/08-176.htm; ETHICS COMM. OF THE KY. JUDICIARY, FORMAL JUDICIAL ETHICS OP. JE-119 (2010), *available at* http://www.courts.ky.gov/NR/rdonlyres/FA22C251-1987-4AD9-999B-A326794CD62E/0/JE119.pdf [hereinafter KY. OP. JE-119]; OKLA. JUDICIAL ETHICS ADVISORY PANEL, JUDICIAL ETHICS OP. 2011-3, 2011 WL 3715149 (July 6, 2011) [hereinafter OKLA. OP. 2011-3]; FLA. SUP. CT., JUDICIAL ETHICS ADVISORY COMM., OP. 2010-5 (2010), *available at* http://www.jud6.org/LegalCommunity/LegalPractice/opinions/jeacopinions/2010/2010-05.html [hereinafter FLA. OP. 2010-5]; and MASS. JUD. ETHICS COMM., CJE OP. No. 2011-6, *available at* http://www.mass.gov/courts/sjc/cje/2011-6n.html [hereinafter MASS. OP. 2011-6].

and Kentucky, extend this ruling to permit a judge to "friend"[14] an attorney who appears in proceedings before the judge, while other states, including California, Florida, Massachusetts, and Oklahoma, are officially opposed to the practice and forbid judges from making online connections with any attorney who may appear before the judge in court.[15]

These state committees base their opinions on two main ethical duties imposed by the state's Code of Judicial Conduct, in combination with other lesser duties. The most important ethical considerations concern a judge's duty to remain impartial and to avoid the appearance of outside influence or impropriety.

### *A. Maintaining Impartiality*

The second canon of the Model Code of Judicial Conduct holds that a judge "shall perform the duties of judicial office impartially, competently, and diligently."[16] Although this blanket rule is relatively vague, various rules refine the definition. In particular, Rule 2.10 states that a judge shall not make any public comment that might "reasonably be expected" to affect the outcome of a pending or impending proceeding before the judge, or that would impair or substantially interfere with the fairness of the trial or hearing.[17] A judge's comments on a social networking site would implicate, and likely violate, this duty if they in any way relate to the status of an ongoing or upcoming trial.

Similarly, Rule 2.9 prohibits the judge from ex parte communications with any party to the litigation.[18] This rule is

---

[14] The verb "friend" refers to the act of issuing or accepting a "friend request" from a social network user, particularly on Facebook. While the ethics opinions cited in this Article consider the ramifications for judges who *accept* friend requests, the same rules likely apply for judges who wish to issue a friend request to another user.

[15] *See* OHIO OP. 2010-7; KY. OP. JE-119; OKLA. OP. 2011-3; FLA. OP. 2010-5.

[16] *See* MODEL CODE OF JUDICIAL CONDUCT Canon 2.

[17] *See* MODEL CODE OF JUDICIAL CONDUCT Canon 2, R. 2.10.

[18] *See* MODEL CODE OF JUDICIAL CONDUCT Canon 2, R. 2.9 (stating that a judge "shall not initiate, permit, or consider ex parte communications, or consider other communications made to the judge outside the presence of the parties or their lawyers, concerning a pending or impending matter," except when circumstances

particularly problematic for judges who accept or extend "friend requests" to or from a party to the pending or ongoing proceeding before the judge, as the judge could then use the social networking site as a means of communication to the exclusion of the other parties. In theory, the judge could communicate with the lawyer by sending messages or posting comments relating to the litigation, or by viewing information posted by the attorney on his or her own networking page.

### B. *Avoiding the Appearance of Outside Influence and Impropriety*

All ethics committees to consider the question have noted that the appearance of outside influence and impropriety is a crucial concern in a judge's use of social networking sites. The first canon of the Model Code of Judicial Conduct prescribes that "a judge shall uphold and promote the independence, integrity, and impartiality of the judiciary,"[19] where "independence" is defined as "freedom from influence or controls other than those established by law."[20] Rule 1.2 holds that "a judge shall act at all times in a manner that promotes public confidence in the . . . judiciary, and shall avoid impropriety and the appearance of impropriety."[21] Similarly, Rule 2.4 holds that a judge "shall not convey or permit others to convey the impression that any person or organization is in a position to influence the judge."[22] As several advisory opinions demonstrate, the designation of the lawyer, party, or witness as a "friend" of the judge implicates these ethical rules in the social networking context.

As the term implies, a "friendship" between a judge and a party or counsel to a proceeding before the judge may constitute an improper and unethical relationship, because the friend could potentially leverage this personal connection to improperly influence the judge. Most committees resolve this issue by noting that terms such as "friend," "follower," or "fan" are terms of art used by the site and

---

require, such as for scheduling or administrative purposes).

[19] *See* MODEL CODE OF JUDICIAL CONDUCT Canon 1.

[20] *See* MODEL CODE OF JUDICIAL CONDUCT, TERMINOLOGY.

[21] *See* MODEL CODE OF JUDICIAL CONDUCT Canon 1, R. 1.2.

[22] *See* MODEL CODE OF JUDICIAL CONDUCT Canon 2, R. 2.4(C).

thus should not be understood in the typical sense of the word.[23] For example, the Ethics Committee of the Kentucky Judiciary explained that a listing as a "friend" or equivalent does not, by itself, "reasonably convey to others an impression that such persons are in a special position to influence the judge."[24] Under this view, the use of the term "friend" should not be sufficient to implicate an improper relationship.

Ethics committees in Florida, California, and Oklahoma disagree with this point. Although the Florida committee was split on the issue, the majority "believe[s] that allowing lawyers who practice before a judge to appear as 'friends' on the judge's Facebook page . . . conveys the impression to the public what Canon 2B prohibits, i.e., that the lawyer is in a special position to influence the judge."[25] In other words, the Florida committee majority is not swayed by the argument that "friend" is merely a term of art; rather, it believes that the term connotes an actual friendship or relationship. Thus, Florida prohibits judges from becoming "friends" with any attorney who may litigate in a proceeding before the judge.[26] Advisory committees in Massachusetts and California recently adopted this rule, and similarly ban judges from accepting friend requests from parties who may appear before the judge in court. Oklahoma also agrees, and even extends the rule to people who "regularly appear in court in an adversarial role," including "social workers, law enforcement officers, or others."[27]

In determining how a judge could avoid the appearance of impropriety, the grievance committee of the Ohio Supreme Court explained that a judge should disqualify himself or herself from a proceeding "when the judge's social networking relationship with a lawyer creates bias or prejudice concerning the lawyer for a party."[28] However, the committee noted that there is no bright-line rule for

---

[23] KY. OP. JE-119.

[24] *Id.*

[25] FLA. SUP. CT., JUDICIAL ETHICS ADVISORY COMM., OP. 2010-06 (2010), *available at* http://www.jud6.org/LegalCommunity/LegalPractice/opinions/jeacopinions/2010/2010-06.html.

[26] *Id.*

[27] OKLA. OP. 2011-3.

[28] OHIO OP. 2010-7.

determining when the online relationship reaches such a level. Instead, the committee explained that "the mere existence of a friendship between a judge and an attorney or between a judge and a party will not disqualify the judge from cases involving that attorney or party."[29] The Kentucky committee noted that judges should be "mindful" of whether online "connections" rise to the level of a "close social relationship," whether viewed alone or in combination with other facts.[30] Yet the committee declined to outline factors to consider in determining whether the relationship is a "close" one.

## IV. PROBLEM AREAS AND THE NEED FOR CAUTION

While all state ethics committees have opined that judges may generally use social networking sites, the opinions caution that judges may not take the same liberties as laymen and that judges must obey strict requirements in order for their use to comply with the Model Code of Judicial Conduct. These requirements generally restrict the judge's participation in comments, messages, status updates, pictures, and research of parties and witnesses.

### *A. Comments, Messages, and Status Updates*

Whether a judge posts his or her own "status update" or comments on the post or status of a friend, ethics committees suggest that the judge should absolutely refrain from making any comments related to a current or pending proceeding before the judge. As the Ohio advisory committee cautioned, "A judge should not make comments on a social networking site about any matters pending before the judge—not to a party, not to a counsel for a party, not to anyone."[31] The committees thus construe this requirement quite strictly: if a judge participates in social networking, the judge should never write about or comment on proceedings pending before that judge.

Disregarding this advice may warrant a public reprimand or other disciplinary action. In one recent case, a North Carolina judge was

---

[29] *Id.*
[30] KY. OP. JE-119.
[31] OHIO OP. 2010-7.

disciplined after "friending" a defense attorney involved in a child custody proceeding before the judge and commenting on counsel's posts regarding the proceeding.[32] While the parties were discussing settlement agreements, the judge posted a status update that he had "two good parents to choose from," and that he "[felt] that he [would] be back in court." Shortly thereafter, the judge wrote that he "was in his last day of trial" and posted a note on defense counsel's wall stating "you are in your last day of trial."[33] The North Carolina Judicial Standards Commission publicly reprimanded the judge for this conduct, proclaiming that the judge failed "to act at all times in a manner that promotes public confidence in the integrity and impartiality of the judiciary" as required by the code of judicial conduct.[34]

### B. *Posting Pictures and Commenting on Pictures Posted by Others*

Although not as controversial as posting comments or status updates, judges should still use discretion in posting pictures or commenting on pictures posted by others. The Kentucky advisory committee noted that judges are held to a higher standard than the average person, and therefore must avoid the appearance of impropriety in posting pictures or commenting on pictures posted by others.[35] Yet beyond specifically prohibiting the posting of explicit material, the standards and expectations for members of the judiciary are unclear. General bounds of professional responsibility would suggest that all professionals—lawyers and judges alike—should not post pictures depicting improper or unprofessional behavior, or comment on inappropriate pictures posted by others. However, judges should also be aware that publicly commenting on pictures posted by an attorney involved in a proceeding before the judge could appear

---

[32] *Public Reprimand of B. Carlton Terry*, N.C. Judicial Standards Comm., Inquiry No. 08-234 (2009), *available at* http://www.aoc.state.nc.us/www/public/coa/jsc/publicreprimands/jsc08-234.pdf.

[33] *Id.*

[34] *Id.*

[35] KY. OP. JE-119, at 4.

improper. Members of the judiciary should therefore refrain from commenting on any picture posted by opposing counsel and should carefully select their own pictures to post in accordance with their desired professional image.

### C. *Researching Parties and Witnesses*

The advisory opinions suggest that judges must refrain from using Facebook or other social networking sites to monitor the activity of parties or witnesses, or to obtain information that exceeds the scope of the facts presented in the case at issue. As one committee explicitly stated, "a judge should not view a party's or witnesses' pages on a social networking site and should not use social networking sites to obtain information regarding the matter before the judge."[36] This advice is closely tied with the prohibition against "Googling" parties to a pending proceeding before the judge, which is an accepted ground for disciplinary action.[37]

In short, as the Supreme Court of Ohio ethics committee suggested, "A judge should be aware of the contents of his or her social networking page, be familiar with the social networking site policies and privacy controls, and be prudent in all interactions on a social networking site."[38]

## CONCLUSION

The few states to consider the ethics of making "friends" with judges on Facebook are divided on whether a judge may accept a "friend request" from a lawyer who has appeared or will appear before the judge in court. Ethics committees in those states that permit the practice express the need for caution in social networking interactions, because a judge must structure online communications to avoid the appearance of impropriety or undue influence. Although the majority of states have yet to address this issue, judges in all states should approach social networking cautiously in order to avoid

---

[36] OHIO OP. 2010-7.

[37] *See, e.g.*, *Public Reprimand of B. Carlton Terry*, N.C. Judicial Standards Comm., Inquiry No. 08-234 (2009).

[38] OHIO OP. 2010-7.

violating the ethical duties governing the judiciary.

PRACTICE POINTERS

- As most states have yet to decide whether judges may "friend" attorneys who practice before the judge, judges should consider declining friend requests from attorneys who have been or may be involved in a proceeding before the judge.
- Judges who are already "friends" with attorneys involved in active proceedings should consider using privacy settings to restrict the content available to these parties.
- Members of the judiciary should never comment on a social networking site about any pending proceeding, whether in a status update or as a response to another person's post.
- Attorneys should avoid "friending" a judge before whom the attorney has appeared or will likely appear in court.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 3 WINTER 2012

# CHEAPER WATCHES AND COPYRIGHT LAW: NAVIGATING "GRAY MARKETS" AFTER THE SUPREME COURT'S SPLIT IN *COSTCO V. OMEGA, S.A.*

*Parker A. Howell*[*]


Cite as: 7 Wash J.L. Tech. & Arts 237 (2012)[†]
http://digital.law.washington.edu/dspace-law/handle/1773.1/1113

## ABSTRACT

*Some manufacturers seek to prevent unauthorized importation and sale of their foreign-made products, called "gray market" goods or "parallel imports," through copyright law. U.S. copyright law prohibits importation of copyrighted works without the copyright owner's permission. At least one manufacturer, Omega, sought to extend this protection to its watches, a useful product, by affixing copyrighted logos. In* Costco v. Omega, S.A., *Omega claimed Costco violated its distribution right by selling the watches in the U.S., while Costco contended that a first sale abroad had extinguished Omega's rights. The case reached the U.S. Supreme Court, which affirmed by an evenly divided court the Ninth Circuit's holding that the first-sale doctrine does not apply when products are initially made and sold abroad. The Court's decision suggested that copyright law might offer businesses a potent method to fight parallel importation. However, on remand the district court granted summary judgment to Costco on the rationale that applying a copyrighted logo to an otherwise useful product constituted copyright*

---

[*] Parker A. Howell, University of Washington School of Law, Class of 2012. Thank you to Professor Robert Gomulkiewicz, Nathan Ferguson of Wilson Sonsini Goodrich & Rosati, and student editors Aurora Wilson and Heather Griffith for your valuable feedback.

[†] Originally published April 10, 2012. Revised April 19, 2012.

*"misuse." While Omega has appealed, the district court's decision suggests a critical limitation on producers' use of copyright to protect utilitarian goods from unauthorized importation and sale.*

TABLE OF CONTENTS

## INTRODUCTION

Authentic, name-brand goods acquired abroad and sold domestically at a discount have found their way into (or onto) the hands of U.S. consumers for decades—undercutting companies' attempts to maintain separate pricing structures for their products in domestic and foreign markets. Globalization and the historical strength of the U.S. dollar have fueled the trend of retailers relying on these "parallel imports," also known as "gray market" goods, as a cost-effective way to source products.[1]

Although federal tariff and trademark laws prohibit certain parallel imports, these doctrines offer limited remedies. For example, trademark law only forbids unauthorized importation of products that bear material differences from their domestic counterparts. Some companies have turned to copyright law in an attempt to stop parallel imports.

In one high-profile case, Swiss watch maker Omega S.A. probed the boundaries of the statutory copyright distribution right by attempting to create a backdoor trademark.[2] Omega affixed copyrighted logos to its foreign-made wristwatches and claimed copyright infringement when wholesaler Costco, an unauthorized Omega retailer, sold the watches in the U.S. In the ensuing litigation in federal court, Costco claimed two defenses: the first-sale doctrine and copyright "misuse." Although Costco lost on the first argument before the U.S. Supreme Court in *Costco Wholesale Corp. v. Omega S.A.*,[3] it prevailed on the latter upon remand.[4]

First, the Supreme Court voted 4-4 to affirm without explanation that the first-sale defense does not apply when goods are made abroad and imported into the U.S.[5] The first-sale doctrine

---

[1] *See* Weil Ceramics & Glass, Inc. v. Dash, 878 F.2d 659, 662 n.1 (3d Cir. 1989) (noting that the term "gray market" implies "a nefarious undertaking by the importer" but has become "commonly accepted and employed").

[2] Omega S.A. v. Costco Wholesale Corp., 541 F.2d 982 (9th Cir. 2008), *aff'd sub nom. by an equally divided court*, Costco Wholesale Corp. v. Omega S.A., 131 S.Ct. 565 (2010).

[3] Costco Wholesale Corp. v. Omega S.A., 131 S.Ct. 565 (2010).

[4] Omega S.A., v. Costco Wholesale Corp., No. 04-05443, slip op. at 4 (C.D. Cal. Nov. 9, 2011).

[5] *Costco*, 131 S.Ct. 565.

generally prevents a copyright owner from restricting later resale or distribution by a purchaser or recipient of a lawful copy of a work.[6] Prior to the *Omega* case, it was unsettled whether the U.S. first-sale doctrine provided a defense to claims of infringement arising from importation or sale of foreign-made goods without the copyright holder's permission. At least one federal appeals court had suggested that the statutory defense generally limits producers' rights,[7] while other federal courts ruled that an initial, lawful sale abroad did not exculpate a later seller.[8] Most of these cases involved "traditional" copyrighted works—products that fixed creative expression in a tangible form, such as textbooks.[9]

Many commentators expected the United States Supreme Court to resolve this issue when it granted certiorari to the Ninth Circuit.[10] However, the Court did not provide an explanation of its decision. The Second Circuit in *John Wiley & Sons, Inc. v. Kirtsaeng*, an analogous case, subsequently reached a similar conclusion, construing the first-sale defense as inapplicable to foreign-made products, even after a lawful U.S. sale.[11] These decisions suggested that importers and retailers should not rely on a first-sale defense to allegations of copyright infringement stemming from parallel imports. The Supreme Court has granted certiorari in *John Wiley & Sons.*[12]

Second, Costco later prevailed with a different argument—copyright misuse—revealing a key potential limit on the extent of copyright protection against parallel importation for certain useful

---

[6] *See* 17 U.S.C. § 109(a) (2011).

[7] *See* Sebastian Int'l, Inc. v. Consumer Contacts (PTY) Ltd., 847 F.2d 1093, 1098 n.1 (3d Cir. 1988).

[8] *See, e.g.*, Omega S.A. v. Costco Wholesale Corp., 541 F.2d 982, 987 (9th Cir. 2008); Pearson Educ. v. Liu, 656 F. Supp. 2d 407, 412 (S.D.N.Y. 2009); CBS v. Scorpio Music Distrib., 596 F. Supp. 47, 49 (E.D. Pa. 1983), *aff'd without opinion*, 738 F.2d 424 (3d Cir. 1984).

[9] *See, e.g.*, *Pearson*, 656 F. Supp. 2d 407 (textbooks). *Cf.* Quality King Distributors, Inc. v. L'anza Research Int'l, Inc., 523 U.S. 135 (1998) (copyrighted hair product labels).

[10] Costco Wholesale Corp. v. Omega S.A., 131 S.Ct. 2089 (2010).

[11] John Wiley & Sons, Inc., v. Kirtsaeng, 654 F.3d 210 (2d Cir. 2011), *cert. granted*, 2012 WL 1252751 (U.S. April 16, 2012) (No. 11697).

[12] *Id*.

goods. On remand, the district court granted summary judgment based on Omega's "misuse" of copyright doctrine.[13] Today, it remains unclear to what extent, if any, U.S. copyright law forbids unauthorized importation and sale of useful goods bearing such copyrighted designs.

This Article discusses the background of parallel importation and the legality of parallel importation under both trademark and copyright regimes. It examines how courts have analyzed whether the first-sale defense applies to unauthorized importation of foreign-made products, culminating with the *Costco* and *John Wiley & Sons* decisions. This Article also explores the implications of the *Omega* district court's grant of summary judgment against Omega based on the doctrine of copyright misuse. This Article suggests that trademark law, not copyright, is the proper analytical paradigm for addressing gray market goods. Further, this Article argues that goods merely adorned with a copyrighted logo, such as the watches at issue in *Omega*, are improper subjects for copyright import restrictions; applying copyright law to these products raises antitrust concerns and creates an undesirable form of backdoor trademark that may be remedied by application of the copyright misuse doctrine.[14]

## I. BACKGROUND ON GRAY MARKET PRODUCTS

The propriety of gray market products has become the subject of both legal and economic debate over the last three decades. The Supreme Court defines a gray market product as a "foreign-manufactured good, bearing a valid United States trademark that is imported without the consent of the United States trademark

---

[13] Omega S.A., v. Costco Wholesale Corp., No. 04-05443, slip op. at 4 (C.D. Cal. Nov. 9, 2011).

[14] Courts and commentators have used the term "backdoor" to describe perceived attempts to create intellectual property protection for a work that would not otherwise qualify for that type of protection. *See, e.g.*, Smith & Hawken, Ltd. v. Gardendance, Inc., No. 04-1664, 2005 WL 1806369, at *3 (N.D. Cal. July 28, 2005). *See generally* Viva R. Moffat, *Mutant Copyrights and Backdoor Patents: The Problem of Overlapping Intellectual Property Protection*, 19 BERKELEY TECH. L.J. 1473, 1515 (2004).

holder."[15] The term also applies to genuine copyrighted goods imported without authorization.[16] At least three situations may create incentives to import gray market goods: currency fluctuations, production and cost differences between nations, and price discrimination in different markets and territories.[17] The ease of international Internet commerce further aids such transactions.[18] Parallel imports today may represent billions of dollars' worth of trade in the U.S. economy.[19] One industry estimate pegged the value of gray market information technology products sold in 2007 at $58 billion or more.[20]

The prevalence of parallel importation springs from producers' natural inclination toward price discrimination.[21] By selling products at different prices in different geographic markets, a business can attempt to maximize profits by charging a higher price in wealthier nations. This strategy may backfire, however, when third parties take advantage of price discrepancies by buying products cheaply in a poorer market and reselling them in a richer area—a process known as "arbitrage."[22]

---

[15] K Mart Corp. v. Cartier, 486 U.S. 281, 285 (1988).

[16] *See generally* 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 8.12(B)(6) (Matthew Bender, rev. ed. 2011).

[17] Joseph Karl Grant, *The Graying of the American Manufacturing Economy: Gray Markets, Parallel Importation, and a Tort Law Approach*, 88 OR. L. REV. 1139, 1142-45 (2009).

[18] *See* Vartan J. Saravia, *Shades of Gray: The Internet Market of Copyrighted Goods and A Call for the Expansion of the First-Sale Doctrine*, 15 SW. J. INT'L L. 383, 383-84, 413 (2009).

[19] Andrew B. Chen, *Shopping the Gray Market: The Aftermath of the Supreme Court's Decision in Quality King Distributors, Inc. v. L'anza Research International, Inc.*, 19 LOY. L.A. ENT. L.J. 573 (1999).

[20] KPMG LLP, EFFECTIVE CHANNEL MANAGEMENT IS CRITICAL IN COMBATING THE GRAY MARKET AND INCREASING TECHNOLOGY COMPANIES' BOTTOM LINE 30 (2008), *available at* http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/Effective-channel-management-gray-market.pdf.

[21] Michael Stockalper, Note and Comment, *Is There A Foreign "Right" of Price Discrimination Under United States Copyright Law? An Examination of the First-Sale Doctrine As Applied to Gray-Market Goods*, 20 DEPAUL J. ART, TECH. & INTELL. PROP. L. 513, 518-21 (2010); *see also* Saravia, *supra* note 18, at 387.

[22] Stockalper, *supra* note 21, at 518-21; *see also* Saravia, *supra* note 18, at

Depending on one's perspective, this phenomenon may represent large-scale savings for U.S. consumers or a loss of potential revenue by producers who desire to engage in market segmentation.[23] Proponents of gray market goods argue that sale of products obtained at lower prices to U.S. consumers at prices below what authorized retailers would charge "prevent[s] price gouging by manufacturers and promot[es] consumer welfare."[24] Critics, primarily producers who believe they lose revenues through parallel importation, contend that gray market products "harm their goodwill and brand image," allowing gray marketers to free ride on their advertising and marketing.[25] Whether to allow manufacturers protection against parallel importation under various intellectual property theories thus reflects the underlying theme of IP law as a "balance between providing incentives through exclusive rights and encouraging use of information through free access to creative works."[26]

## II. LEGAL REGIMES FOR CONTROL OF PARALLEL IMPORTATION

Business interests have turned to a variety of legal doctrines in an effort to prevent unauthorized importation of products. Federal tariff and trademark law provide the traditional lines of defense, as discussed in Section A.[27] However, U.S. copyright law might offer companies like Omega an additional tool to control unauthorized importation of products, as discussed in Section B. Section C describes how courts have taken different approaches as to whether the U.S. first-sale doctrine limits copyright protection against unauthorized importation of copyrighted works when those

---

384.

[23] *See generally* Saravia, *supra* note 18, at 396; Grant, *supra* note 17, at 1187.

[24] Lynda J. Oswald, *Statutory and Judicial Approaches to Gray Market Goods: The "Material Differences" Standard*, 95 KY. L.J. 107, 109 (2007).

[25] *Id*.

[26] *See* David W. Barnes, *The Incentives/Access Tradeoff*, 9 NW. J. TECH. & INTELL. PROP. 96 (2010).

[27] In addition, companies may have remedies under state law, such as tortious interference with contracts and unfair competition. *See* Grant, *supra* note 17, at 1184-86.

products are made abroad.

### *A. Traditional Lines of Defense: Tariff and Trademark Law*

Although both the federal Tariff Act of 1930[28] and the Lanham Act[29] offer businesses some protection against parallel importation, these doctrines provide limited remedies. Both laws allow manufacturers to stop infringing goods at the border.[30]

The Tariff Act bars unauthorized importation of a good "that bears a trademark owned by a citizen of . . . the United States and is registered in the U.S. Patent and Trademark Office."[31] But this "extraordinary protection" is limited to U.S. trademark owners that have no corporate affiliation with the foreign manufacturer of a given product.[32] Thus, a company cannot stop importation of its own products on the gray market.

Trademark law provides another avenue of protection, although it also does not bar unauthorized importation of every product. The Lanham Act prohibits importation of merchandise that is likely to cause confusion among consumers about who produced a product or where it was made.[33] Trademark law "has been an effective legal means for businesses to ban gray market goods."[34] However, the Act only applies to products that are "physically and materially different" from domestic products.[35] Thus, trademark law generally does not apply when a company sells or authorizes distribution of identical versions of its trademarked good in

---

[28] Tariff Act of 1930 (Smoot-Hawley Act), § 526, 19 U.S.C. § 1526 (2006).

[29] Lanham Act, § 42, 15 U.S.C. § 1124 (2006).

[30] *See* 5 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 29:37 (4th ed. 2011).

[31] 19 U.S.C. § 1526 (2006).

[32] K Mart Corp. v. Cartier, Inc., 486 U.S. 281, 295 (1988) (Brennan, J., concurring).

[33] *See* 15 U.S.C. § 1124. *See also* American Circuit Breaker Corp. v. Oregon Breakers Inc., 406 F.3d 577 (9th Cir. 2005).

[34] 2 CORPORATE COUNSEL'S GUIDE TO DISTRIBUTION COUNSELING § 19:3 (2011).

[35] *Id*.

different markets, some of which become parallel imports.[36] Some producers turn to copyright law in an attempt to stop parallel importation of products lacking material differences.

### *B. Attempts to Use Copyright Law as a Means to Prevent Parallel Importation*

Following a string of federal court decisions, copyright law may hold the greatest promise for producers of traditional copyrighted works, such as books, and for a small subset of companies that make utilitarian products yet want to maintain international market segmentation (*i.e.*, Omega).[37] Provisions of U.S. copyright law prohibit the importation of unauthorized copyrighted goods, offering producers a method to circumvent the market-differentiation requirement of trademark law. Under the Copyright Act, the unauthorized sale of imported products "probably is copyright infringement if the imported work was originally manufactured abroad, even if such manufacture were done with the permission of the copyright proprietor."[38] The reasons for this, however, are complex: they involve the Act's ambiguous statutory language and judicial concerns about applying U.S. copyright law extraterritorially.

Unlike the source-identification function of trademark law, copyright law aims to foster scientific progress by giving creators limited rights to their works.[39] In order to qualify for copyright protection, goods must be original works of authorship exhibiting a modicum of creativity that have been fixed in a tangible medium.[40]

---

[36] *See, e.g.*, Dan-Foam A/S v. Brand Named Beds, LLC, 500 F. Supp. 2d 296, (S.D.N.Y. 2007); Swatch S.A. v. New City, Inc., 454 F. Supp. 2d 1245, 1249 (S.D. Fla. 2006) ("Under what has been called the 'first sale' or 'exhaustion' doctrine, the trademark protections of the Lanham Act are exhausted after the trademark owner's first sale of its product."); Iberia Foods Corp. v. Romeo, 150 F.3d 298 (3d Cir. 1998).

[37] *See* Saravia, *supra* note 18, at 394-95.

[38] 4 LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMPETITION, TRADEMARKS & MONOPOLIES § 22:53 (4th ed. 2010).

[39] *See* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984).

[40] *See* 17 U.S.C. § 102 (2011).

Works of craftsmanship, such as watches, that are "useful" are not protectable, although separable ornamental features may be copyrightable.[41] While the most commonly discussed right is against unapproved copying, the Act also prohibits unauthorized public *distribution* of works.[42]

Congress amended the Copyright Act in 1976 to prohibit importation of copyrighted works into the country under certain circumstances.[43] Section 602 states that importing copies or phonorecords "acquired outside" the U.S. "without the authority of the owner of copyright" constitutes "infringement of the exclusive right to distribute copies or phonorecords" under § 106.[44] Yet while copyright law provides a variety of benefits for a potential litigant concerned about parallel imports,[45] alleged infringers have claimed a defense: the first-sale doctrine.

### *C. Courts Reach Different Conclusions about the Contours of the First-Sale Doctrine as Applied to Parallel Imports*

Debate among courts and commentators centers on whether and to what extent Congress intended the first-sale doctrine of

---

[41] 2 WILLIAM F. PATRY, PATRY ON COPYRIGHT § 3:148 (2011). *See, e.g.*, Severin Montres, Ltd. v. Yidah Watch Co., 997 F. Supp. 1262, 1265 (C.D. Cal. 1997), *aff'd*, 165 F.3d 917 (9th Cir. 1998).

[42] *See* 17 U.S.C. § 106(3) (2011); *see generally* 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 8.11-.12 (Matthew Bender, rev. ed. 2011). The distribution right "is a necessary supplement to the production right in order fully to protect the copyright owner"; otherwise, a creator could control production of copies but not the initial release of the work. *Id.*

[43] *See* 17 U.S.C. § 602 (2011).

[44] *Id*. Section 602 makes violations actionable under 17 U.S.C. § 501 (2011). The law provides exemptions for single copies imported for personal use and importation for scholarly, educational, or religious purposes rather than for private gain. § 602(3). U.S. Customs and Border Protection lacks authority to stop importation of "lawfully made" copies at the border, but people claiming a copyright interest in a particular work may pay a fee to be notified of the importation of articles that appear to be copies of the work. § 602(b).

[45] Copyright infringers are subject to joint and several liability, allowing a copyright owner to decide which infringer to sue. Chen, *supra* note 19, at 598. A copyright claim does not hinge on an infringer's actual knowledge of the violation. *Id.* And a plaintiff need not show intent to infringe. *Id.*

§109 to limit §§ 106(3) and 602(a). The first-sale doctrine generally provides that the initial sale of a creative work exhausts the copyright holder's interest in controlling subsequent sales of that product.[46] This gives creators a say in how their works are initially sold while fostering free enterprise by removing such restrictions for later sales. Courts have specifically wrestled with whether goods must be manufactured in the U.S. in order to be "lawfully made" for purposes of the statute and thus to take advantage of the defense, as described in Section 1.[47] Section 2 describes the influential concurring opinion of Justice Ginsburg that limited the first-sale defense to U.S.-made copies. The Supreme Court in *Costco* ultimately affirmed without explanation that the first-sale doctrine is limited to U.S.-made copies, as described in Section 3.

1. Early Decisions Suggest a Distinction in Application of the Doctrine to U.S.- and Foreign-Made Goods

In a series of early decisions considering application of the first-sale doctrine to parallel imports, federal courts distinguished between U.S.- and foreign-made products. The U.S. District Court for the Eastern District of Pennsylvania held that the first-sale doctrine did not extinguish copyright owners' interest in foreign-made imported goods.[48] In *Columbia Broadcasting System, Inc. v. Scorpio Music Distributors, Inc.*, Columbia Broadcasting sued after Scorpio purchased from a third-party importer approximately 6,000 audio recordings. Columbia Broadcasting owned the copyrights to the recordings, which were only authorized for production and sale in the Philippines.[49] The defendant pleaded the first-sale doctrine. But the court held that allowing the defense

---

[46] *See* 17 U.S.C. § 109(a) (2011). *See generally* 4 WILLIAM F. PATRY, PATRY ON COPYRIGHT § 13:16 (2011).

[47] *See, e.g.*, John Wiley & Sons, Inc. v. Kirtsaeng, 654 F.3d 210, 219 (2d Cir. 2011), *cert. granted*, 2012 WL 1252751 (U.S. April 16, 2012) (No. 11-697).

[48] Columbia Broadcasting System, Inc. v. Scorpio Music Distributors, Inc. 569 F. Supp. 47, 49 (E.D. Pa. 1983), *aff'd sub nom.* CBS, Inc. v. Scorpio Music Distributors, Inc., 738 F.2d 421 (3d Cir. 1984).

[49] *Id*. at 47.

would conflict with explicit Congressional will.[50] On appeal, the Third Circuit affirmed without discussion.[51]

However, in *Sebastian Int'l, Inc. v. Consumer Contacts (PTY) Ltd.*,[52] the Third Circuit held that a beauty supply manufacturer, "having sold its goods with copyrighted labels to foreign distributors . . . is barred by the first sale doctrine from establishing infringement through an unauthorized importation."[53] As products bearing copyrighted labels—rather than objects themselves protected by copyright—the goods at issue in *Sebastian* were more like the watches at issue in *Omega* than the phonorecords sold in *Scorpio*. The court vacated a preliminary order "enjoining defendants from distributing within the United States products that plaintiff had manufactured *in this country* and then exported."[54] While the court discussed cases from other circuits that limited the application of the first-sale defense to U.S.-made copies, it "confess[ed] some uneasiness with this construction of 'lawfully made' because it does not fit comfortably within the scheme of the Copyright Act."[55] The court reasoned that "[w]hen Congress considered the place of manufacture to be important, . . . the statutory language clearly expresses that concern."[56]

2. Justice Ginsburg Suggests in Dicta that the First-Sale Doctrine Applies Only to "Round-Trip" Importation, a Position Adopted by Subsequent Courts

Nearly a decade later, the Supreme Court held in the landmark case of *Quality King Distributors, Inc. v. L'anza Research International, Inc.* that the first-sale doctrine limits §§ 106 and 602

---

[50] *Id*. at 49.

[51] *CBS*, 738 F.2d 421.

[52] Sebastian Int'l, Inc. v. Consumer Contacts (PTY) Ltd., 847 F.2d 1093 (3d Cir. 1988) (emphasis added).

[53] *Id*. at 1094.

[54] *Id*. (emphasis added).

[55] *Id*. at 1098 n.1.

[56] *Id*. The court pointed to 17 U.S.C. § 601(a) (2011), which prohibits importation or distribution in the U.S. of copies consisting of certain English literary material unless the material was "manufactured in the United States or Canada." *Id.*

when goods are made in the U.S. with copyrighted labels, shipped abroad, and later re-imported.[57] Respondent L'anza, a hair-care product manufacturer, charged foreign distributors significantly less for the same products bearing copyrighted labels than it charged in the U.S. The products themselves were not copyrighted, only the labels. Petitioner Quality King Distributors purchased L'anza products made in the U.S. and imported from a distributor in Malta, and L'anza sued for copyright infringement. The Ninth Circuit affirmed a judgment finding that Quality King had infringed L'anza's copyright under § 602(a) by importing the products without authorization, deciding that § 109 provided no defense.[58]

The Supreme Court reversed, ruling that § 602 did not categorically bar unauthorized importation of copyrighted materials.[59] The Court held:

> [S]ince § 602(a) merely provides that unauthorized importation is an infringement of an exclusive right "under section 106," and since that limited right does not encompass resales by lawful owners, the literal text of § 602(a) is simply inapplicable to both domestic and foreign owners of [copyrighted] products who decide to import them and resell them in the United States.[60]

However, in a brief (though now well-known) concurring opinion, Justice Ruth Bader Ginsburg, joined by no other justice, noted that *Quality King* "involves a 'round trip' journey, travel of the copies in question from the United States to places abroad, then back again."[61] Justice Ginsburg stated that the Court did not "resolve cases in which the allegedly infringing imports were manufactured abroad" and then imported into the U.S.[62] She cited

---

[57] Quality King Distributors, Inc. v. L'anza Research Int'l, Inc., 523 U.S. 135 (1998).

[58] *Id*. at 135.

[59] *Id*. at 154 (Ginsburg, J., concurring).

[60] *Id.* at 145.

[61] *Id.* at 154 (Ginsburg, J., concurring).

[62] *Id.*

a treatise for the proposition that "provisions of Title 17 do not apply extraterritorially unless expressly so stated, hence the words 'lawfully made under this title' in the 'first sale' provision, 17 U.S.C. § 109(a), must mean 'lawfully made in the United States.'"[63]

Courts in later cases have relied on this concurrence to support their view that the first-sale doctrine does not limit § 602 when copies are produced abroad. For example, in 2009 the U.S. District Court for the Southern District of New York looked to the *Quality King* dicta to hold that the first sale doctrine does not protect importers of foreign-made textbooks designated for sale abroad and later imported into the U.S.[64] The plaintiffs in *Pearson Education, Inc., v. Liu*, copyright holders who published textbooks throughout the world and to whom authors had granted exclusive rights to reproduce and distribute the works within the U.S., sued the defendant importers for importing textbooks without authorization and selling them online.[65] The *Pearson* court noted that "nothing in § 109(a) or the history, purposes, and policies of the first-sale doctrine, limits the doctrine to copies of a work" made in the U.S.[66] The court would likely have held that the first-sale doctrine provides a defense for works made abroad and imported, if the district court "were to limit its consideration to the traditional tools of statutory interpretation."[67] However, the court concluded the dicta in *Quality King* addressing a similar situation required it to defer to the Supreme Court.[68] The court reasoned that "[w]hen the Supreme Court addresses an unsettled question of federal law in unanimous dicta, respect for the Supreme Court as an institution and the dedicated jurists who serve on it mandates deference in all but the most exceptional circumstances."[69]

---

[63] *Id*. at 154 (Ginsburg, J., concurring) (citing WILLIAM F. PATRY, COPYRIGHT LAW AND PRACTICE 166-170 (1997 Supp.)).

[64] Pearson Education, Inc. v. Liu, 656 F. Supp .2d 407 (S.D.N.Y. 2009).

[65] *Id.* at 408-09.

[66] *Id.* at 410.

[67] *Id.* at 411.

[68] *Id.* at 416.

[69] *Id*.

### 3. The Ninth Circuit Adopts a Restrictive Interpretation of the First-Sale Doctrine in *Omega*, which the Supreme Court Affirms

The *Omega* case again propelled gray market goods before the Supreme Court, resulting in the Court's split affirmance that the first-sale defense does not apply to foreign-made goods. The case began with sale of Swiss-made, Omega-brand watches by Costco, a privately held warehouse club based in Washington State, without Omega's authorization. Costco purchased Seamaster watches bearing the copyrighted "Omega Globe Design" logo engraved on the back from a New York company.[70] That company had purchased the watches from unidentified third parties, who had bought them from authorized distributors abroad. Costco sold the watches for just $1,299.99, compared with a suggested retail price of $1,995.00.[71] Omega's legal department had suggested adding the design, copyrighted in 2003, after authorized U.S. dealers complained about Costco's sale of the watches.[72] The watchmaker stated in a newsletter that "the purpose of this lawsuit was to 'stem the tide of the grey market.'"[73]

Omega sued Costco in 2004 for copyright infringement under 17 U.S.C. §§ 106(2) (right to prepare derivative works) and 106(3) (right to distribute works) and moved for summary judgment.[74] In a cross-motion, Costco claimed the first-sale defense. The district court ruled for Costco without explanation.[75]

The Ninth Circuit reversed, holding that § 109(a) provided no defense because the first-sale doctrine only applies to copyrighted goods made in the U.S.[76] The court distinguished its decisions prior to *Quality King* by stating that *Quality King* applied only to

---

[70] Omega S.A. v. Costco Wholesale Corp., 541 F.3d 982, 983-84 (9th Cir. 2008).

[71] Omega S.A., v. Costco Wholesale Corp., No. 04-05443, slip op. at 1 (C.D. Cal. Nov. 9, 2011).

[72] *Id.* at 2.

[73] *Id*.

[74] *Omega*, 541 F.3d at 984.

[75] *Id*.

[76] *Id.* at 990.

"'round trip' importation."[77] The court's rationale centered on concerns that reading "lawfully made" to include copies made outside the U.S. would apply U.S. copyright law extraterritorially.[78] The *Omega* court reasoned that for the first-sale doctrine to apply, copies of a work must be "lawfully made" under the Act; hence, applying the doctrine to foreign-made works would "ascribe legality" under the Act to "conduct that occurs entirely outside the United States, notwithstanding the absence of a clear expression of congressional intent in favor of extraterritoriality."[79]

The *Omega* court did not reach the issue of whether, as pre-*Quality King* Ninth Circuit decisions held, a lawful U.S. sale enables the first-sale defense for later transactions.[80] The court reasoned that there was no question the foreign-made copies were sold in the U.S. without Omega's authorization.[81]

The Supreme Court granted certiorari in April 2010. International companies ranging from Amazon.com to Intel signed on in support of Costco's position as amici.[82] Although commentators expected the High Court to settle this issue, an equally divided Court affirmed the Ninth Circuit without explanation. The split occurred because of the recusal of newly appointed Justice Elena Kagan, who had argued against certiorari while serving as solicitor general for the Obama Administration.[83]

---

[77] *Id*. at 985-87 (citing Denbicare U.S.A. Inc. v. Toys "R" Us, Inc., 84 F.3d 1143 (9th Cir. 1996); Parfums Givenchy, Inc. v. Drug Emporium, Inc., 38 F.3d 477 (9th Cir. 1994); BMG Music v. Perez, 952 F.2d 318 (9th Cir. 1991)).

[78] *Id*. at 988-99.

[79] *Id*. at 988 (citations omitted).

[80] *Id*. at 990 (citing *Denbicare*, 84 F.3d 1143, 1145-46 (9th Cir. 1996)).

[81] *Id*.

[82] *See, e.g.*, Brief for eBay, Inc., et al. as Amici Curiae Supporting Petitioners, Costco Wholesale Corp. v. Omega, S.A., 130 S.Ct. 2089 (2010), 2010 WL 2770102.

[83] *See* Brief of the United States as Amici Curiae Supporting Respondents, Costco Wholesale Corp. v. Omega, S.A., 130 S.Ct. 2089 (2010), 2010 WL 3512773.

## III. IMPLICATIONS OF THE *COSTCO* COURT'S SPLIT AFFIRMANCE FOR THE SCOPE OF THE FIRST-SALE DEFENSE

While some commentators opine that the Supreme Court's lack of concrete language on whether the first-sale defense applies to foreign-made copyrighted goods creates uncertainty for businesses,[84] the affirmance follows a decades-long trend post-*Quality King* of reading the doctrine narrowly. The Supreme Court's ruling implicitly validates the Ninth Circuit's rationale—that extraterritoriality concerns prevent application of the first-sale defense to infringement claims involving certain foreign-made goods. However, the absence of a written decision by the Court leaves unanswered the justices' current views on the limits of § 109(a), especially on whether a lawful sale in the U.S. extinguishes a copyright owner's distribution right.

While it is possible that other circuits to consider this issue might diverge from the Ninth Circuit's interpretation that the first-sale doctrine is inapplicable to certain foreign-made goods, such an event seems unlikely following the Supreme Court's action.[85] For example, the Supreme Court's split decision in *Lotus Dev. Corp. v. Borland Int'l, Inc*., affirmed that copyright law does not cover menu command hierarchy for computer software because it is a "method of operation," effectively deciding that issue.[86]

Nonetheless, importers and retailers who may deal in parallel imports should be cautious about importing, purchasing, and selling "traditional" copyrighted works, such as books or phonorecords. As discussed in Section A below, such caution is especially warranted in light of a recent Second Circuit opinion

---

[84] *See, e.g.*, Joe Mullin, *Patent Litigation Weekly: Costco v. Omega — The Patent Angle*, CORPORATE COUNSEL (ONLINE), Sept. 13, 2010.

[85] *But see* BRIAN T. YEH, APPLICABILITY OF THE COPYRIGHT LAW'S FIRST SALE DOCTRINE TO IMPORTED GOODS MANUFACTURED ABROAD: COSTCO WHOLESALE CORP. V. OMEGA S.A. (Jan. 6, 2011) (suggesting that "other circuits are free to issue opinions that agree or conflict with the Ninth Circuit"), *available at* http://ipmall.info/hosted_resources/crs/R41422_100921.pdf.

[86] Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807, 807 (1st Cir. 1995) *aff'd by an equally divided court*, 516 U.S. 233 (1996).

mirroring, and perhaps extending, the Ninth Circuit's reasoning.[87] However, as discussed in Section B, analysis of the rationales underlying copyright law suggests that trademark law would be better suited to govern parallel importation. Furthermore, the district court's holding on remand in *Omega* suggests that there may be important limits to the application of copyright law to certain useful articles, as discussed below in Section IV.

### *A. The Second Circuit Follows* Costco *by Limiting the First-Sale Defense*

In a 2011 case analogous to *Pearson*, the Second Circuit in *John Wiley & Sons, Inc. v. Kirtsaeng* ruled squarely that the language of § 109(a)—"lawfully made under this title"—limits the first-sale doctrine to cases where the good in question was manufactured within the U.S.[88] This decision reinforces the Supreme Court's ruling in *Costco*, although the Court will have another opportunity to speak on this issue following its grant of certiorari in April 2012.

The plaintiff, a publisher of textbooks, sued a student who sold textbooks obtained abroad in the U.S. on commercial sites such as eBay.com, alleging copyright infringement.[89] Kirtsaeng argued the first-sale doctrine as a defense, but the trial court held that the doctrine did not apply because the goods were made abroad.[90]

The Second Circuit affirmed, relying primarily on the *Quality King* dicta.[91] The court "freely acknowledge[d] that this is a particularly difficult question of statutory construction in light of the ambiguous language of § 109(a)," but stated that its "holding is supported by the structure of Title 17 as well as the Supreme Court's opinion in *Quality King*."[92] The court noted that "Congress

---

[87] *See* John Wiley & Sons, Inc., v. Kirtsaeng, 654 F.3d 210 (2d Cir. 2011), *cert. granted*, 2012 WL 1252751 (U.S. April 16, 2012) (No. 11-697)

[88] *Id*. at 221.

[89] *Id*. at 213.

[90] *Id*. at 214.

[91] *Id*. at 220-22.

[92] *Id*. at 222.

is of course able to correct our judgment."[93] Notably, the court explicitly stated that the first-sale doctrine *never* applies to sales of foreign-made copies in the U.S., even after a lawful domestic sale; it distinguished contrary Ninth Circuit precedent.[94] In his petition for certiorari, Kirtsaeng argues that *John Wiley & Sons* thus represents "*Costco* on steroids."[95]

In a dissenting opinion reminiscent of the Third Circuit's reasoning in *Sebastian*, District Judge J. Garvan Murtha argued that the first-sale defense should apply because "[t]he statutory text does not refer to a place of manufacture" and instead focuses on "whether a particular copy was manufacture[d] lawfully under [T]itle 17."[96] Hence, Judge Murtha reasoned, "a copy authorized by the U.S. rightsholder is lawful under U.S. copyright law."[97] Judge Murtha also argued that such a reading of § 109(a) does not render § 602 meaningless because it will apply to "copies of a work not lawfully manufactured under [T]itle 17 but lawfully manufactured under some other source of law . . . and to copies not in the possession of the 'owner.'"[98]

Despite the arguments raised by this dissent, the Second Circuit's decision in *John Wiley & Sons* further demonstrates that federal appeals courts are unwilling to contradict the *Quality King* dicta, taking the first-sale defense off the table when foreign-made products are imported without the U.S. copyright owner's authorization. However, it remains unclear how the Supreme Court will view the applicability of the first-sale doctrine following a lawful U.S. sale, an issue not addressed in *Costco*.

### *B. Congressional Revision of Federal Intellectual Property Law Would Alleviate Doctrinal Uncertainty*

Court decisions allowing the first-sale defense against even

---

[93] *Id*.

[94] *Id*. at 221.

[95] Petition for Writ of Certiorari, *John Wiley & Sons*, 654 F.3d 210 (No. 11-697), 2012 WL 6098030 at *6.

[96] *John Wiley & Sons*, 654 F.3d at 226 (citation omitted).

[97] *Id*.

[98] *Id*. at 228.

foreign-made goods would better accord with the policies underlying copyright law and would likely have beneficial economic effects. However, any changes in this area should be left to Congress, not the federal courts.

A ruling contrary to *Omega* and *John Wiley & Sons* would best fit with copyright doctrine, as pointed out by Judge Murtha, the dissenter in the latter case: "Once the copyright holder has controlled the terms on which the work enters the market, i.e., the purpose of the distribution right, 'the policy favoring a copyright monopoly for authors gives way to the policy opposing restraints of trade and restraints on alienation.'"[99] Judge Murtha aptly states that "[g]ranting a copyright holder unlimited power to control all commercial activities involving copies of her work would create high transaction costs and lead to uncertainty in the secondary market."[100] However, federal courts are constrained by valid competing concerns about extraterritorial application of U.S. copyright law, as demonstrated by the Ninth Circuit's *Omega* decision. [101]

A high court ruling allowing the first-sale defense to claims of unauthorized importation of foreign-made goods also could reduce incentives for producers to move manufacturing abroad. The Ninth Circuit conceded that its interpretation might "encourage U.S. copyright owners to outsource the manufacturing of copies."[102]

This incongruity derives from the fact that copyright law is the incorrect doctrine for use in preventing parallel importation—at least for utilitarian products—because it is meant to grant creators a limited monopoly over their works, not to serve the source-identification function of trademarks. Revision of the Lanham Act would be a better means to accomplish checks on the gray market, if Congress desires.[103]

---

[99] *Id.* at 227 (Murtha, J., dissenting) (quoting Pearson Educ., Inc. v. Liu, 656 F. Supp. 2d 407, 409 (S.D.N.Y. 2009)).

[100] *Id*.

[101] *See generally* 7 WILLIAM F. PATRY, PATRY ON COPYRIGHT § 25:86 (2011).

[102] Omega S.A. v. Costco Wholesale Corp., 541 F.3d 982, 989 (9th Cir. 2008).

[103] *Cf.* Chen, *supra* note 19, at 598 (arguing for revision of the Copyright Act).

Enacting legislative reform to intellectual property regimes may be difficult. Yet Congress has acted to remedy such intellectual property issues with international implications following high-profile cases. For example, Congress enacted a statute prohibiting shipping components of a patented invention abroad to avoid patent protection in the wake of *Deepsouth Packing Co. v. Laitram Corp*.[104]

## IV. HOW FAR WILL COURTS EXTEND PROTECTION TO COPYRIGHTED LOGOS ON UTILITARIAN ARTICLES?

Despite Omega's victory in the Supreme Court, on remand the district court suggested that there are limits to the applicability of the copyright distribution right as a mechanism to prevent parallel importation. The U.S. District Court for the Central District of California in November 2011 granted summary judgment for defendant Costco, reasoning that Omega's strategy of emblazoning its watches with a copyrighted logo to segment international markets constituted "misuse" of its copyright.[105] Omega has appealed this decision to the Ninth Circuit.[106] Thus, it remains unclear to what extent producers may subject otherwise utilitarian products, such as watches, to import and distribution restrictions by adorning them with copyrighted designs. The district court's decision, while perhaps extending the misuse doctrine, arrives at the proper result: copyright law should not be employed as a form of backdoor trademark.

As discussed in Section A, copyright import protection based on designs added to otherwise utilitarian goods raises antitrust concerns. Section B discusses the *Omega* district court's application of the copyright misuse doctrine. Section C argues that such application of the misuse doctrine will remedy overreaching

---

[104] Deepsouth Packing Co. v. Laitram Corp., 406 U.S. 518 (1972). *See* 35 U.S.C. § 271(f)(1) (2006).

[105] Omega S.A., v. Costco Wholesale Corp., No. 04-05443, slip op. at 3-4 (C.D. Cal. Nov. 9, 2011).

[106] Notice of Appeal, Omega S.A. v. Costco Wholesale Corp., No. 11-57137 (Dec. 9, 2011).

by a subset of copyright holders who seek to prevent parallel importation.

### *A. Extension of Copyright Protection to Otherwise Utilitarian Articles Implicates Antitrust Concerns*

Depending on how the Ninth Circuit views the district court's application of the copyright misuse doctrine, producers might restrict importation after *Costco* by affixing copyrighted logos to a host of everyday items that otherwise would not qualify for copyright protection. Granting the owners of copyrighted logos attached to otherwise non-copyrightable articles exclusive distribution rights in the U.S. implicates antitrust concerns because it gives copyright holders a broader monopoly than allowed by Congress.[107] This is evident from comparing the facts of *Omega* to cases involving traditional copyrighted works.

In general, many consumer products do not qualify for copyright protection because they are not "original works of authorship" for purposes of 17 U.S.C. § 101.[108] In addition, certain three-dimensional products with designs that might qualify for protection as "pictorial, graphic, or sculptural" works, such as watches, are not protectable unless the aesthetic aspects are separable from the utilitarian aspects.[109] Omega added the copyrighted design, which was about 1/8 of an inch in size, to the *underside* of its watches specifically to combat parallel

---

[107] *See* Andrew Spillane, *Combatting Gray Markets: A Copyright-Protected Distribution Right or a Sherman Act Violation?*, MARQUETTE UNIVERSITY LAW SCHOOL FACULTY BLOG (July 20, 2011), http://law.marquette.edu/facultyblog/2011/07/20/combatting-gray-markets-a-copyright-protected-distribution-right-or-a-sherman-act-violation.

[108] *See* 1 MELLVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.03 (Matthew Bender, rev. ed. 2011).

[109] For pictorial, graphic, or sculptural works, a "'useful article' is an article having an intrinsic utilitarian function that is not merely to portray the appearance of the article or to convey information.'" 17 U.S.C. § 101 (2006). *See generally* 2 WILLIAM F. PATRY, PATRY ON COPYRIGHT § 3:124-3:154 (2011).

importation.[110] The watches themselves did not qualify for copyright protection because they were useful articles.[111]

While the Ninth Circuit in *Omega* and the Second Circuit in *John Wiley & Sons* reached similar results, the cases are distinguishable based on the nature of the products at issue. The imported textbooks in *John Wiley & Sons* were copyrighted works in their entirety. However, in *Omega*, the watches merely bore a copyrighted logo. The Ninth Circuit's decision arguably blurred the line between copyright and trademark law by validating Omega's strategy of bringing a useful product within the protective embrace of § 602(a) by placing a small copyrighted logo on it. The Supreme Court granted certiorari on the narrow question of the applicability if the first-sale doctrine, leaving lower courts to address the issue of copyright misuse.

A similar issue arose in the pharmaceutical industry. Drug companies whose products had been protected by patent sued makers of generic versions of the drugs for using copyrighted language on their ingredient labels.[112] The Second Circuit stated:

> [C]ommercial labeling is clearly copyrightable . . . it has been recognized that the "danger lurking in copyright protection for labels is that the tail threatens to wag the dog-proprietors at times seize on copyright protection for the label in order to leverage their thin copyright protection over the text . . . on the label into a monopoly on the typically uncopyrightable product to which it is attached."[113]

---

[110] *See* Omega S.A., v. Costco Wholesale Corp., No. 04-05443, slip op. at 3-4 (C.D. Cal. Nov. 9, 2011).

[111] *See generally* Severin Montres Ltd. v. Yidah Watch Co., 997 F. Supp. 1262, 1265 (C.D. Cal. 1997) (stating watches are "useful article[s] with an intrinsic utilitarian function" not entitled to copyright protection unless the design is "separable from the utilitarian aspects").

[112] *See* SmithKline Beecham Consumer Healthcare, L.P. v. Watson Pharmaceuticals, Inc., 211 F.3d 21, 23-24 (2d Cir. 2000).

[113] *Id*. at 29 n.5 (citations omitted). The Second Circuit ultimately concluded that the Food and Drug Administration requirements that the labels bear certain information precluded a copyright infringement action, but noted that copyright holders may still pursue copyright claims against potential

In similar fashion, businesses that pursue Omega's copyright strategy circumvent the Lanham Act's requirement that products sold abroad bear material differences from their domestic counterparts to qualify for import protection.

Proponents of such increased copyright protection might point to both the *Omega* decision and the Supreme Court's willingness to extend import control rights to holders of copyrighted hair product labels in *Quality King*. The Supreme Court called *Quality King* an "unusual copyright case" because the plaintiff did not claim "anyone has made unauthorized copies of its copyrighted labels."[114] Rather, the plaintiff was "primarily interested in protecting the integrity of its method of marketing the products to which the labels are affixed."[115]

Yet critics could cite the same passage, in which the *Quality King* Court stated that the "labels themselves have only a *limited creative component*."[116] Consumers might "suffer from this disparity, as it allows the copyright owner to charge them higher prices for a copyrighted logo that may add nothing to the value of the goods."[117]

### *B. On Remand, the District Court Grants Summary Judgment for Costco Based on Omega's Copyright "Misuse"*

The *Omega* district court on remand employed the misuse doctrine to prevent such an unjust result. The court took issue with Omega's legal strategy to protect its authorized distributors of the watches, stating that Omega "used the defensive shield of copyright law as an offensive sword."[118]

---

infringers in other circumstances, such as the use of the copyrighted material in non-labeling advertisements.

[114] Quality King Distributors, Inc. v. L'anza Research Int'l, Inc., 523 U.S. 135, 140 (1998).

[115] *Id*.

[116] *Id*. (emphasis added).

[117] James L. Bikoff, David K. Heasley & Michael T. Delaney, Costco v. Omega*: The 'Foreign First Sale' Debate*, 28 NO. 17 WESTLAW J. COMPUTER AND INTERNET 1, 3 (2011).

[118] Omega S.A., v. Costco Wholesale Corp., No. 04-05443, slip op. at 2 (C.D. Cal. Nov. 9, 2011).

In general, copyright misuse is a defense to claims of infringement premised on a plaintiff's attempts to "extend the scope of [the copyright] monopoly" that constitutes a "violation of the antitrust laws."[119] Applying the Ninth Circuit's copyright misuse test, the court stated that misuse occurs when a "copyright is being used in a manner violative of the public policy embodied in the grant of copyright."[120] In addition, the misuse defense "prevents copyright holders from leveraging their limited monopoly and allow[s] them to control areas outside of their monopoly."[121] The court held that Omega, having conceded that a purpose of the design was to control importation, "misused its copyright . . . by leveraging its limited monopoly in being able to control the importation of that design to control the importation of its Seamaster watches."[122]

The court found unpersuasive that the design might have multiple purposes, such as promoting "creativity and aesthetics" and increasing the value of the watches.[123] The court held that "those aspects of the design are protected by its copyright and are not a defense to copyright misuse."[124] Ultimately, copyright misuse is an "equitable defense to copyright infringement, the contours of which are still being defined."[125] The doctrine of copyright misuse, although controversial, presents an avenue for courts to address this doctrinal rift.[126]

---

[119] 4 MELLVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 13.09(A)(1)(a) (Matthew Bender, rev. ed. 2011).

[120] *Omega*, No. 04-05443, slip op. at 3 (citing Lasercomb Am., Inc. v. Reynolds, 911 F.2d 970, 978 (4th Cir. 1990)).

[121] *Id*. at 4.

[122] *Id*.

[123] *Id*.

[124] *Id*.

[125] *Id.* (citing MDY Industries, LLC, v. Blizzard Entertainment, Inc., 629 F.3d 928, 941 (9th Cir. 2010)).

[126] *Compare* Defendant Costco Wholesale Corporation's Memorandum of Points and Authorities in Opposition to Omega's Motion for Partial Summary Judgment, Omega S.A v. Costco Wholesale Corp., No. 04-5443 (C.D. Cal. Sept. 1, 2011), 2011 WL 5122927, *with* Plaintiff's Memorandum of Points and Authorities in Opposition to Defendant's Motion for Summary Judgment, Omega S.A v. Costco Wholesale Corp., No. 04-5443 (C.D. Cal. Sept. 1, 2011), 2011 WL 5122926. *See generally* 5 WILLIAM F. PATRY, PATRY ON COPYRIGHT

### *C. The Copyright Misuse Doctrine Offers a Remedy to Overbroad Use of Copyright in the Parallel Importation Context*

The analytical mismatch between the policies underlying copyright law and efforts to control parallel importation is evidenced by extension of import protection in *Costco* to utilitarian goods bearing contrived copyrighted works. Omega likely did not (or could not) bring a trademark claim because there was no evidence that Swiss-made Omegas sold by Costco would cause confusion among consumers about the watches' origin or producer. While the copyrighted logo may have served as an indication of the watches' source, this consumer-protection function should be left to trademark law.

In the absence of misuse doctrine, "overlapping" copyright and trademark protection "implicates the 'delicate balance' of the copyright bargain by interfering with the incentive structure established by Congress."[127] Overlapping protection contradicts the rationale underlying copyright law—fostering creativity by giving authors limited-duration rights to control reproduction and distribution of their creations—and creates a form of backdoor trademark.[128] In contrast, federal trademark law aims to protect consumers by helping them to identify the source (and thus the quality) of goods and to protect businesses by reducing the potential for confusion among competing products.[129] Furthermore, "patent and copyright law confer certain exclusive property rights, whereas trademark law protects only against similar uses that are likely to cause confusion."[130]

---

§ 17:128 (2011).

[127] Moffat, *supra* note 14, at 1516 (quoting Stewart v. Abend, 495 U.S. 207, 230 (1990)).

[128] *See, e.g.*, Mazer v. Stein, 347 U.S. 201, 219 (1954). *See also* SmithKline Beecham Consumer Healthcare v. Watson Pharmaceuticals, Inc., 211 F.3d 21, 29 n.5 (2d Cir. 2000).

[129] *See* Moseley v. V Secret Catalogue, Inc., 537 U.S. 418, 428 (2003) (citations omitted).

[130] Curtis A. Bradley, *Territorial Intellectual Property Rights in an Age of Globalism*, 37 VA. J. INT'L L. 505, 538 (1997).

Prior to the district court's order, it appeared producers could supplement their trademarks with copyrighted logos, a situation that could ultimately harm consumers by granting broad exclusive import rights not limited by the necessity of showing likelihood of consumer confusion. Application of the misuse doctrine would prevent companies from unfairly extending copyright protection to maintain parallel distribution arrangements.

## CONCLUSION

The law governing parallel imports remains in flux, presenting a challenge both for businesses looking to maintain their international pricing strategies and importers and retailers who wish to supply products obtained at a discount overseas. The Supreme Court in *Costco* effectively decided that the copyright first-sale doctrine does not provide a defense to claims of infringement related to unauthorized *importation* of foreign-made copyrighted works. Yet it is unresolved whether the Supreme Court in *John Wiley & Sons* will follow past Ninth Circuit decisions in allowing the first-sale defense after a lawful U.S. sale of a copyrighted work. Furthermore, the *Omega* district court's application of the copyright misuse doctrine offers a limitation on businesses' ability to restrict importation merely by affixing small copyrighted designs to otherwise utilitarian products. It remains to be seen whether higher federal courts accept this application of the misuse doctrine.

## PRACTICE POINTERS

*For Defendants:*

- Importers and retailers should carefully source products and take steps to verify their supply chains to avoid unexpected copyright liability for selling gray market goods. The first-sale doctrine probably will not provide a defense against infringement claims arising from importation of goods made abroad, although it is unclear whether a lawful U.S. sale enables the first-sale doctrine for later transactions.

- Retailers should avoid purchasing directly from unknown foreign distributors. Purchase from a third-party importer in the U.S. might insulate a party from liability under § 602(a), at least in the Ninth Circuit. For example, Costco waived an argument that its purchase of the watches from a third-party supplier (who had in turn purchased the watches from an importer) shielded it from *import* liability by failing to raise the issue in its opening brief before the Ninth Circuit. Yet a retailer still might face §106(3) liability for unauthorized distribution.

*For Plaintiffs:*

- Manufacturers who want to enforce price discrimination should consider a variety of legal theories to stop parallel importation, such as trademark, contract, and tort. However, they should be aware that making foreign copies "materially different" may be difficult, and perhaps considered anticompetitive.
- Producers who want to enforce price discrimination might consider marking products with copyrighted logos, like the Omega symbol on the watches sold by Costco, in order to potentially bring those products under U.S. copyright law's import restrictions. This strategy is not proven, however, especially in light of the *Omega* district court's application of the equitable doctrine of copyright "misuse" to grant summary judgment for Costco.
- When possible under antitrust laws, manufacturers who want to enforce price discrimination should include prohibitions on resale in licensing and distribution agreements to create a breach of contract claim against suppliers of parallel imports.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 3 WINTER 2012

# LOADED QUESTION: EXAMINING LOADABLE KERNEL MODULES UNDER THE GENERAL PUBLIC LICENSE V2

*Curt Blake and Joseph Probst* [*]


Cite as: 7 Wash J.L. Tech. & Arts 265 (2012)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1115

## ABSTRACT

*This Article examines the intersection of Linux loadable kernel modules and the license under which Linux is distributed, the General Public License (GPL) Version 2. Section I of this Article discusses ambiguous terms contained within the GPL and various interpretations of these ambiguities. Next, Section II analyzes the changing scope of legal protection for computer software, particularly as it pertains to derivative works and as applied to loadable kernel modules. Section III highlights provisions contained within the GPL that may attempt to reach beyond a traditional works analysis and examines these provisions in light of recent developments at the intersection of contract law and intellectual property licensing.*

---

[*] Curt Blake, University of Washington School of Law, Class of 1983. Thanks to Joseph Probst for collaborating with me on this paper, to Robert Gomulkiewicz for helping get a fellow old guy published, and to my wife Kelli and my children Gavin and Anna for keeping things fun.

Joseph Probst, University of Washington School of Law, Class of 2012. Thank you to Curt Blake for the collaborative efforts leading to this paper, to Professor Robert Gomulkiewicz for providing me with the inspiration to further analyze the legal protection of computer software, and to my family for their enduring love and support.

TABLE OF CONTENTS

## INTRODUCTION

As manufacturers increasingly rely on embedded devices[1] to incorporate greater levels of intelligence into embedded systems,[2] demand has grown for the software required to operate these embedded devices. Embedded devices are used in common products like cellular phones, digital cameras, automobiles, and medical instruments. Demand for inexpensive, small operating systems to run these devices has grown as the price of memory and microprocessors has fallen, and the desire for "smart" functions in a variety of devices has risen. The Linux operating system caters to this demand, boasting a smaller footprint than Windows and, due to its open source heritage, a very attractive price tag. The increasing popularity of Linux has generated a need for software that facilitates interaction between the Linux operating system kernel and the specific hardware of the embedded device. Often, the solution takes the form of loadable kernel modules, such as device drivers, which communicate between a piece of hardware and the underlying Linux kernel.[3]

---

[1] *See, e.g.*, *Embedded System*, NETRINO: EMBEDDED SYSTEMS GLOSSARY, http://www.netrino.com/Embedded-Systems/Glossary-E#embedded_system (last visited January 17, 2012). An embedded system is a computer system designed to do one or a few dedicated and/or specific functions, often with real-time computing constraints. It is *embedded* as part of a complete device, which often includes hardware and mechanical parts. By contrast, a general-purpose computer, such as a personal computer (PC), is designed to be flexible and to meet a wide range of end-user needs. Embedded systems control many devices in common use today.

[2] *See, e.g.*, *id.* Embedded systems span all aspects of modern life and there are many examples of their use. Telecommunications systems employ numerous embedded systems from telephone switches for the network to mobile phones at the end-user. Computer networking uses dedicated routers and network bridges to route data. Consumer electronics include personal digital assistants (PDAs), mp3 players, mobile phones, videogame consoles, digital cameras, DVD players, GPS receivers, and printers. Many household appliances, such as microwave ovens, washing machines and dishwashers, are including embedded systems to provide flexibility, efficiency and features. Advanced HVAC systems use networked thermostats to more accurately and efficiently control temperature that can change by time of day and season. Home automation uses wired- and wireless-networking that can be used to control lights, climate, security, audio/visual, surveillance, etc., all of which use embedded devices for sensing and controlling.

[3] ALESSANDRO RUBINI & JONATHAN CORBERT, LINUX DEVICE DRIVERS (2d ed. 2001), *available at* http://www.xml.com/ldd/chapter/book/index.html.

Unfortunately for many developers, the legal consequences of linking to Linux kernels are unsettled. Uncertainty in this area exerts a chilling effect on the development of embedded devices. Developers who have created proven functions for embedded devices running on non-Linux operating systems want to port those functions to embedded devices running on the Linux operating system. At the same time, manufacturers of embedded devices want to use their trusted software partners as they develop their next generation of products in a Linux-centric world. Uncertainty regarding the legal consequences of linking proprietary software to a device running the Linux kernel makes it difficult for developers of proprietary software and embedded devices to reach agreement.

The reason for this uncertainty is the General Public License (GPL),[4] the license to which those using, modifying, or distributing Linux are bound.[5] Several of the key terms used throughout the GPL are poorly defined or used inconsistently.[6] When the ambiguity in these terms is combined with the evolving scope of protection afforded to computer programs by judicial interpretations of the Copyright Act, module developers are unable to properly ascertain the extent of their rights and restrictions.[7]

This Article first analyzes the special case of loadable kernel modules under a narrow interpretation of Section 2 of the GPL, under which the GPL's "copyleft" requirements only apply to works which would be derivative works under the Copyright Act. Next, the Article examines alternate interpretations of Section 2(b) and other provisions contained throughout the GPL that may attempt to extend the copyleft restrictions beyond the scope of a traditional derivative works analysis. Finally, the Article considers these provisions in light of recent Ninth Circuit cases examining the intersection of contract law and intellectual property licensing. The Article concludes that

---

[4] All references to the GPL are to GPL version 2, because Linux is licensed under this version, and is therefore the most popular version of the license.

[5] Sapna Kumar, *Enforcing the GNU GPL*, 2006 U. ILL. J.L. TECH. & POL'Y 1, 10 (2006).

[6] *See generally* Robert W. Gomulkiewicz, *De-Bugging Open Source Software Licensing*, 64 U. PITT. L. REV. 75, 83-92 (2002).

[7] *See, e.g.*, Jeremy Andrews, *Linux: The GPL and Binary Modules*, KERNEL TRAP, (Dec. 5, 2003, 7:14 AM), http://kerneltrap.org/node/1735.

under recent precedent, software modules linked to the Linux kernel are freely licensable because there is no remedy for a licensee's failure to follow the GPL's terms.

## I. OBLIGATIONS UNDER THE GPL

The GPL is commonly known as a "strong copyleft" license—meaning that any derivative work created from a GPL-licensed code, no matter how insignificant the contribution, must also be licensed under the same terms of the GPL license.[8] However, ambiguities in the language of GPL Section 2 give rise to multiple possible interpretations of how far this copyleft provision reaches.

Under a "copyleft" license, "downstream licensees, no matter how far removed from the original licensor, are [] bound by the key GPL terms,"[9] including the requirement to license any derivative work at no charge to third parties. Section 2 of the GPL is one of the key provisions implementing these copyleft requirements. Section 2 states:

> You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions . . . b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License. . . .[10]

It is uncertain how far the obligations of this provision actually reach. The first sentence of Section 2, quoted above, allows for

---

[8] John Tsai, *For Better or Worse: Introducing the GNU General Public License Version 3*, 23 BERKELEY TECH. L.J. 547, 551 (2008).

[9] *Id.*

[10] Free Software Foundation, *GNU General Public License Version* 2, GNU OPERATING SYSTEM, http://www.gnu.org/licenses/gpl-2.0.html [hereinafter GPL v2].Section 3 further requires that the licensee provide access to the source code of the distributed program. GPL v2, Section 3.

modifications that would form a "work based on the Program." However, Section 2(b) requires that the GPL be extended to "any [distributed] work . . . that in whole or in part contains or is derived from the Program or any part thereof." Furthermore, the subsequent sentences of Section 2 use various other terms to describe the result of modifications, including "modified files," "modified program," and "modified work."[11] This use of disparate terms clouds the true effect of the provision.

The first step in untangling Section 2 of the GPL is to understand the scope of a "work based on the Program." Section 0 of the GPL states that "a 'work based on the Program' means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language."[12] A common interpretation of this language is that the term "work based on the Program" is directly linked to the concept of derivative works under copyright law and therefore equivalent in scope.[13] Advocates of this interpretation point to the first clause of the sentence, which limits the definition to "the Program or any derivative work under copyright law."[14] The second clause, which is arguably broader, would then simply be an "interpretive explanation . . . [which] gives an indication of what the GPL drafters thought, hoped, or may argue in a dispute is the meaning of the term 'derivative works' under copyright law."[15] Thus, because the definition directly incorporates and hinges upon an existing, statutorily-defined legal concept, any subsequent elaboration is not sufficient to alter this concept and can be viewed as a statement

---

[11] GPL v2, Section 2. *See also* Lothar Determann, *Dangerous Liasons – Software Combinations as Derivative Works? Distribution, Installation, and Execution of Linked Programs under Copyright Law, Commercial Licenses, and the GPL*, 21 BERKELEY TECH. L.J. 1421, 1487-88 (2006).

[12] GPL v2, Section 0.

[13] Gomulkiewicz, *supra* note 6, at 89. *See also* Michael F. Morgan, *The Cathedral and the Bizarre: An Examination of the "Viral" Aspects of the GPL*, 27 J. MARSHALL J. COMPUTER & INFO. L. 349, 390 (2010) (stating that "the GPL.v3 seems to make it clear that certain terminology used in the GPL is intended to have the same scope as the term 'derivative work' under copyright law" and pointing to the GPL.v3 definition of the term "modify").

[14] GPL v2, Section 0.

[15] Determann, *supra* note 11, at 1487.

of opinion.[16] Therefore, a "work based on the Program" would mean a derivative work as defined by the Copyright Act.

The second step in understanding Section 2 is to note that the conditions set forth in 2(a), (b), and (c) ("the lettered conditions") "apply to the modified work as a whole."[17] Here, the "modified work as a whole" appears to refer to the "work based on the Program" authorized by the first sentence of Section 2.[18] If this phrase is read to be limiting, then references within the lettered conditions to a "modified file," "modified program," or "work that in whole or in part contains or is derived from the Program" can be interpreted as equivalent in scope to the defined term "work based on the Program."[19] Under this interpretation, the copyleft requirements of the lettered conditions would only extend to works that qualify as derivative works under the Copyright Act.

An alternative interpretation of Section 2 of the GPL elevates the importance of the plain meaning of the provisions. For example, the reference in Section 2(b) to a "work that in whole or in part contains . . . the Program," could be construed as including any work that incorporates code from the Program, no matter how insignificant and with no regard to whether the included code would be protectable under the Copyright Act.[20] Thus, "Section 2(b)'s license condition may apply to programs derived from minuscule amounts of code or non-copyrightable code that would not otherwise make the host program a derivative work according to copyright law."[21]

---

[16] *See, e.g.*, Morgan, *supra* note 13, at 394 ("Accordingly, to the extent that the GPL v2 suggests that the copying of any subject matter from 'the Program' necessarily makes a subsequent work a derivative work, that statement is incorrect.")

[17] GPL v2, Section 2.

[18] The second full paragraph of Section 2 later uses the term "work based on the Program" as a direct substitute for the original "modified work as a whole." This direct substitution lends credence to the theory that the requirements of Sections 2(a), (b), and (c) apply to any "work based on the Program."

[19] This implication is fair if the first sentence of the second full paragraph of Section 2, "These requirements . . .," is read as limiting the scope of the lettered conditions only to "modified works." An alternative interpretation of this sentence is that it is non-limiting in the sense that it is simply identifying one category of application out of several.

[20] GPL v2, Section 2; Gomulkiewicz, *supra* note 6, at 90.

[21] Gomulkiewicz, *supra* note 6, at 90. Further textual argument for this

Section II of this Article considers the applicability of the GPL to loadable kernel modules under the first, narrower interpretation discussed above. Section III discusses the second, broader interpretation of the GPL and the effect of recent developments on its possible application to loadable kernel modules.

## II. APPLICABILITY OF THE GPL TO LOADABLE KERNEL MODULES UNDER A DERIVATIVE WORKS ANALYSIS

As discussed above, the GPL attempts to restrict non-GPL software from linking to GPL-licensed programs by asserting the copyright holder's exclusive right to prepare derivative works.[22] This section first provides a brief description of courts' changing attitudes regarding the level of protection afforded to software programs under the Copyright Act, particularly emphasizing the scope of derivative work rights. Next, loadable kernel modules are introduced and analyzed to determine whether they qualify as derivative works.

### *A. The Evolution of the Derivative Works Test Applied to Software*

Over time, the protections afforded software programs and their associated derivative work[23] rights have decreased as courts have better understood the idea-expression dichotomy as applied to software. In particular, as discussed below, courts have expressed willingness to allow copying of software interfaces for purposes of interoperability.

Early court decisions dealing with inter-changeable or inter-operable media, such as *Midway Mfg. Co. v. Artic International*,

---

interpretation contrasts the use of "*the* modified files," "*the* modified program," and "*the* modified work as a whole" with "*any* work that you distribute or publish." *See* GPL v2, Section 2 (emphasis added).

[22] GPL v2, Sections 0, 2 and 3.

[23] A derivative work is defined within the Copyright Act as "a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted." 17 U.S.C. § 101 (2006).

*Inc.*,[24] and *Worlds of Wonder, Inc. v. Veritel Learning Systems, Inc*,[25] "looked at the output of the combination of [the original and the follow-on] works rather than at the works themselves."[26] Under such a broad definition, "courts would struggle to find any add-on components or software that did not create an infringing derivative."[27]

The high point of copyright protection for software was the Third Circuit's decision in *Whelan Assoc., Inc. v. Jaslow Dental Lab, Inc.*[28] In *Whelan*, the plaintiff had provided defendant Jaslow Dental Laboratory with software designed to aid in management of defendant's dental office.[29] After Jaslow developed its own similar office software based upon internal knowledge of Whelan's program, Whelan alleged that the new program infringed the copyright to the original program.[30] Although there were substantial "differences in programming style, in programming structure, in algorithms and data structures," the two programs shared significant "overall structural similarities."[31] The Third Circuit looked beyond the absence of literal, verbatim copying of the source code and instead, by analogy to a literary work, relied upon substantial similarities contained within the structure, sequence, and organization – the "SSO."[32] However, the Third Circuit went even further by suggesting that "the

---

[24] Midway MFG. Co., v. Artic Int'l, Inc., 704 F.2d 1009, 1013-14 (7th Cir. 1983).

[25] Worlds of Wonder, Inc. v. Veritel Learning Sys, Inc., 658 F. Supp. 351 (N.D. Tex. 1986).

[26] Douglas A. Hass, *A Gentlemen's Agreement: Assessing the GNU General Public License and Its Adaptation to Linux*, 6 CHI.-KENT J. INTELL. PROP. 213, 257 (2007).

[27] *Id.*

[28] Whelan Assoc., Inc. v. Jaslow Dental Lab, Inc., 797 F.2d 1222 (3d Cir. 1986).

[29] *Id.* at 1225-27.

[30] *Id.*

[31] *Id.* at 1228.

[32] *Id.* at 1234. ("The copyrights of other literary works can be infringed even when there is no substantial similarity between the works' literal elements. One can violate the copyright of a play or book by copying its plot or plot devices. . . . By analogy to other literary works, it would thus appear that the copyrights of computer programs can be infringed even absent copying of the literal elements of the program.")

sole idea of a computer program is the purpose the program seeks to achieve. In *Whelan*, the purpose was "to aid in the business operations of a dental laboratory." According to the Third Circuit, anything more specific in the program would be considered protectable expression. This approach is quite sweeping in the amount of protection it grants and various commentators have criticized the decision for providing overbroad protection to software.[33]

In the early 1990s, courts began to reduce the scope of copyright protection afforded computer software. As illustrated by the Second Circuit's 1992 decision in *Computer Associates International, Inc. v. Altai, Inc.*,[34] courts began to use more sophisticated analysis, expanding on the idea-expression dichotomy. In *Altai*, the Second Circuit adopted an "abstraction, filtration, comparison" test.[35] Initially, the court divided the program into component parts based upon increasing levels of abstraction. Then, the court filtered out those portions of the software which were unprotectable at each level. In performing the filtering step, the court removed from protection those segments of the code which were a merger of expression and ideas, using "scenes a faire" analysis, as well as those segments of code which were dictated by efficiency concerns.[36] Only after this level of analysis was complete for each level of abstraction did the court compare the two works to determine if, given protectable expression, enough substantial similarity existed to warrant a finding that infringement had occurred. Thus, the *Altai* court removed a significant portion of the protection granted by *Whelen* by denying "protection to specific elements of programs [such as] purely functional features, features dictated by efficiency, and features necessary for compatibility with other programs."[37]

Building on *Altai*, the Ninth Circuit further honed the

---

[33] *See, e.g.*, Peter S. Menell, *An Analysis of the Scope of Copyright Protection for Application Programs*, 41 STAN. L. REV. 1045, 1082-82 (1989).

[34] Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, (2d Cir. 1992).

[35] *Id.* at 706

[36] *Id.* at 706-09. *See also* David C. Tunick, *How to Avoid Infringing the Copyright of a Computer Program: From the Perspective of a Computer Programmer Turned Attorney/Law Professor*, 4 J. INTELL. PROP. L. 49, 56-60 (1996).

[37] Hass, *supra* note 26, at 261.

"abstraction, filtration, comparison" test in deciding two video game cases. In *Sega Enterprises, Ltd. V. Accolade, Inc.*,[38] the court ruled that despite Accolade's reverse engineering of Sega's game console software, its use of only those portions of Sega's software necessary to make its games interoperate with the console was a fair use privileged under § 107 of the Copyright Act.[39] The court stated that "[i]n some circumstances, even the exact set of commands used by the programmer is deemed functional rather than creative for purposes of copyright."[40] Further, "when specific instructions, even though previously copyrighted, are the only and essential means of accomplishing a given task, their later use by another will not amount to infringement."[41] The court ruled that the *Altai* test, when applied to the facts before it, allowed wholesale copying (during reverse engineering) of the console software to the extent necessary to determine which elements of the code which were not protected expression.[42] Furthermore, the court explicitly noted that "the functional requirements for compatibility with the Genesis console . . . are not protected by copyright."[43]

In *Sony Computer Entertainment v. Connectix Corp.*, the Ninth Circuit again ruled reverse engineering to be a fair use.[44] In fact, the court allowed copying of Sony's code not just for the creation of games that interoperate with the plaintiff's game console, but for the creation of software which would at times replace the plaintiff's console software and enable Sony Playstation compatible games to be played on a PC.[45] Again, they ruled that wholesale copying is acceptable when necessary to locate unprotected elements of a software program.[46] In justifying this decision they found not just those elements necessary for interoperability unprotected, but all

---

[38] Sega Enters. LTD. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992).

[39] *Id.* at 1527.

[40] *Id.* at 1524.

[41] *Id.* at 1524 (quoting National Commission on New Technological Uses of Copyrighted Works, Final Report 1 (1979)) (internal quotations omitted).

[42] *Id.* at 1527.

[43] *Id.* at 1522.

[44] Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000).

[45] *Id.* at 608.

[46] *Id.*

"functional elements."[47]

Thus, as courts have become increasingly familiar with computer software, their unmistakable trend is to reduce the scope of protection granted to program code. In particular, as evidenced by the *Altai* filtration step and specific language from both the *Sega* and *Connectix* opinions, code specifically required for interoperability between programs has been explicitly identified as unprotectable, functional code necessitated by efficiency. Thus, courts "have become increasingly solicitous of parties who copy only interfaces of copyrighted software, where the purpose of doing so is to achieve interoperability."[48]

### *B. Applicability of the Modern Derivative Works Test to Loadable Kernel Modules*

To better understand the application of the GPL to loadable kernel modules, a cursory knowledge of the purpose and structure of loadable kernel modules is necessary. The Linux kernel is the core section of Linux code: it is the heart of the operating system and is responsible for allocating system resources such as power, memory, or network connectivity.[49] Loadable kernel modules, on the other hand, are independently developed pieces of code that can be "loaded" into the kernel at runtime (a process also known as "dynamic linking")[50] and that often add new functionality or capabilities.[51] A common example of a loadable kernel module is a device driver, which allows for communication between the kernel

---

[47] *Id.* at 599.

[48] Sean Hogle, *Unauthorized Derivative Source Code*, 18.5 COMPUTER & INTERNET LAW. 1, 6 (2001).

[49] RUBINI, *supra* note 3, at Chapter 1.

[50] This paper deals almost exclusively with the case of dynamically linked kernel modules. For more in depth analysis of the legal ramifications of dynamic vs. static linking of modules see Mitchell Stoltz, *The Penguin Paradox: How the Scope of Derivative Works in Copyright Affects the Effectiveness of the GNU GPL*, 85 B.U. L. REV. 1439 (2005); Tsai, *supra* note 8; and Morgan, *supra* note 13. These references conclude that static linking of a module into the kernel code almost certainly creates a derivative work. They offer differing conclusions with regard to dynamic linking.

[51] RUBINI, *supra* note 3, at Chapter 1.

and a specific piece of hardware.[52] Dynamic linking of kernel modules allows "the original program and the module [to] occupy two separate object code files that can be sold and distributed separately."[53]

Due to their ability to be dynamically linked, loadable kernel modules represent a unique class of software somewhere between the kernel itself and standalone applications. The module resembles an extension of the kernel in the sense that it performs operating system-like functions and communicates with the kernel using the kernel's own internal communication structure.[54] However, a loadable module also contains similarities to standalone applications. Module code is never actually combined with the kernel code, but instead uses a system of interfaces to allow intercommunication between the various active components.[55]

A ruling that standalone applications were derivative works would mean the demise of an entire industry: it is common practice for proprietary applications to run on many different operating systems, including Linux.[56] Fortuitously for application developers, current (though perhaps not pre-*Altai*) decisions have clearly held that the use of software elements necessary for interoperability are unprotected expression.[57] Assuming these elements are the only ones

---

[52] *Id.*

[53] Stoltz, *supra* note 50, at 1449. Later, using a specified module interface, the module can be inserted by reference into the kernel proper and await later invocation of the module's functions. It is important to note, however, that the module code is not literally inserted into the kernel code; Instead, a reference to the module's location within the computer's memory is inserted into the kernel code. Then, when the module functionality is required, the kernel will communicate with the module at the referenced location. After the module functionality is no longer desirable, the module can be unloaded and any references to the module contained within the kernel are eliminated.

[54] RUBINI, *supra* note 3, at Chapter 2.

[55] Hass, *supra* note 26, at 254-55.

[56] *Id.* at 251.

[57] See discussion of *Altai*, *Sega*, and *Connectix* in Section II.A, *supra*; *but see* Edward J. Naughton, *Bionic Revisited: What the Summary Judgment Ruling in* Oracle v. Google *Means for Android and the GPL*, BROWN RUDNICK ALERT, 5-8 (Nov. 2011), *available at* http://www.brownrudnick.com/nr/pdf/alerts/Brown_Rudnick_Bionic_Revisited_Naughton_11-11.pdf (pointing to recent developments in *Oracle v. Google* and arguing that inline functions and variables

borrowed from an operating system in the creation of an application, standalone applications are not derivative works.

With this in mind, distinguishing between standalone applications and kernel modules is arguably a matter of degree and not kind. For instance, a Windows version of Adobe Photoshop cannot run on the Windows operating system without using the Windows-specific system call interface. In the same fashion, the device driver for a video card in a Windows PC cannot communicate with the operating system without using Windows-specific driver interfaces. Thus, both the standalone application and the device driver module are independent pieces of code designed to interact with a specific operating system using specified interface code.

Depending on the desired function and design of a kernel module, the interface between the module and the kernel can range from simple to highly complex and incorporate a significant amount of functional code.[58] Under the logic of *Altai*, *Sega*, and *Connectix*, however, it does not matter how much of the functional interface code a module contains because this code is inherently unprotectable under the Copyright Act. For instance, after noting that certain works more closely track the core intent of the Copyright Act than others, the *Connectix* court stated that "Sony's BIOS [software] lies at a distance from the core because it contains unprotected aspects . . . [w]e consequently accord it a 'lower degree of protection than more traditional literary works.'"[59] Further, the *Sega* court noted that "[u]nder a test that breaks down a computer program into its component subroutines and sub-subroutines and then identifies the idea or core functional element of each . . . many aspects of the program are not protected by copyright."[60] Because these courts

---

cannot be deemed *per se* uncopyrightable and instead must be subjected to a line-by-line analysis.)

[58] *See, e.g.*, Hass, *supra* note 26, at 265 (discussing Linus Torvald's comments on the stability of the Linux API and the changing scope of module functionality) and *id.*, at 255 (discussing a driver facilitating communication between the kernel and a high-speed data networking card, by "copy[ing] required data structures and other function names" from the kernel).

[59] Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 603 (9th Cir. 2000) (quoting Sega Enters. LTD. v. Accolade, Inc., 977 F.2d 1510, 1526 (9th Cir. 1992)).

[60] *Sega*, 977 F.2d at 1525.

specifically identified functional requirements for compatibility as unprotected,[61] use of such unprotectable code should never, by itself, lead to a finding of infringement upon an exclusive right of a copyright holder.

It remains to be seen to what extent courts will be willing to allow copying for the sake of interoperability. For instance, a module that "pervasively incorporates" the underlying data structures or internal communication processes of the kernel may be found to be a derivative work, either because some of the code will be deemed protectable expression or because the module copies non-literal elements of the kernel, such as the structure, sequence, or organization, which are protected under copyright.[62] However, assuming Linux kernel modules only contain the source code or headers necessary to enable efficient interoperability of proprietary code with the Linux Kernel, the modules fall squarely within the protections elucidated by *Altai*, *Sega* and *Connectix* for successful avoidance of classification as a derivative work.

Thus, under the interpretation of Section 2(b) of the GPL set forth above in Section II of this Article, the requirements of the GPL will only extend to those loadable kernel modules that would qualify as derivative works under the Copyright Act. Modules that only incorporate unprotected, functional code necessary for interoperability do not trigger the requirements of the GPL.[63]

## III. APPLICABILITY OF THE GPL BEYOND A DERIVATIVE WORKS ANALYSIS

### *A. Alternative Interpretations of the GPL*

Unfortunately for software developers hoping to create

---

[61] *See id.* at 1522; *Connectix*, 203 F.3d at 603.

[62] Hogle, *supra* note 48, at 5. *See also* Naughton, *supra* note 57, at 8-9 (arguing that Google's attempt to "clean" the GNU C library ("glibc") of copyright protectable material when creating the Android Bionic library failed, in part, because Google did not consider the copyright covering "the overall structure of the API").

[63] This Article will further discuss the implication that this finding has upon various modes of distribution in Section III, *infra*.

proprietary modules that interact with the Linux kernel, certain provisions of the GPL might be interpreted to reach beyond a straightforward derivative works analysis. As discussed in Section II of this Article, *supra*, some commentators have pointed to the plain language of Section 2(b) of the GPL, which requires the GPL to be applied to any work "that in whole or in part contains or is derived from the Program or any part thereof."[64] Thus, reading this phrase literally, a module could be an independent, non-derivative work under copyright law, but still required to be released under the GPL by the express terms of the agreement because it contains "a part" of the Program. Furthermore, later provisions of Section 2 also purport to extend control beyond that of copyright law. In particular, after setting forth the lettered conditions, Section 2 states:

> These requirements [the lettered conditions] apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.
>
> Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.[65]

At first blush this portion of the GPL ("the collective works

---

[64] GPL v2, Section 2(b); *see e.g.* Tsai, *supra* note 8, at 555-56.

[65] GPL v2, Section 2. Section 2 subsequently states: "In addition, mere aggregation of another work not based on the Program with the Program (or a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License."

provision") appears to track copyright law by applying the obligations of the GPL only to derivative works, but it introduces ambiguity by attempting to apply the GPL to non-derivative works which are "reasonably considered independent" if they are distributed "as part of a whole which is a work based on the Program."[66] As discussed above, the definition of the term "work based on the Program" is open to interpretation and as such could be equal to or broader in scope than the concept of derivative works under the Copyright Act.

The GPL further muddies the water by suggesting, through an interpretive gloss, intent to control the distribution of "collective works based on the Program."[67] Once again, the extent of the GPL's reach is unclear due to the combination of statutorily defined terminology[68] with idiosyncratically worded concepts such as a "work based on the Program." However, the net effect of the collective works provision appears to be an attempt extend the GPL's reach beyond the program and its derivative works to any "collective work based on the program" which contains a *modified* GPL-covered program in addition to any number of independent, non-derivative sections, if those independent sections can be considered part of a "modified work as a whole."[69]

In the following sections, this Article discusses the application and possible effects of these ambiguities on various factual scenarios. In particular, each of the provisions introduced above will be assessed in light of several recent Ninth Circuit cases that analyze the intersection of copyright law and contract law. This distinction between contract and copyright law is critical because, in the event the GPL is interpreted as a contract, the remedy for breach, absent a provision enabling injunctive relief, is likely limited to monetary

---

[66] *Id.*

[67] *Id.*

[68] *See* 17 U.S.C § 101 (2010) ("A 'collective work' is a work, such as a periodical issue, anthology, or encyclopedia, in which a number of contributions, constituting separate and independent works in themselves, are assembled into a collective whole").

[69] Section 2 of the GPL also notes that "mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License."

damages.

### *B. Recent Decisions on the Intersection of Copyright Law and Contract Law*

Several recent Ninth Circuit cases have analyzed the license-versus-sale dichotomy and expounded upon the interaction between contract and licensing law. Although these cases are all interpretations of the first-sale doctrine, they have implications on how the Ninth Circuit will enforce software license agreements. The trio of cases—*Vernor v. Autodesk, Inc.*,[70] *UMG Recordings, Inc., v. Augusto*,[71] and *MDY Industries, LLC, v. Blizzard Entertainment, Inc.*[72]—set limits on the availability of copyright infringement actions as a remedy for non-compliance with an agreement, whether styled as a contract or a license.

In *Vernor*, an eBay vendor brought an action seeking a declaratory judgment that he had the legal right to resell copies of Autodesk's software packages.[73] Autodesk claimed that the agreement that accompanied the software (the "software license agreement" or "SLA") was, in fact, a license to use the software under specific conditions, one of which forbade the resale of the software.[74] Vernor alleged that the software had been sold to its first owner, rather than licensed, and therefore the first sale doctrine applied.[75] The *Vernor* court, in holding that Autodesk was entitled to an injunction halting re-sale of its software online, stated:

> [A] software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions. Applying our holding to Autodesk's SLA, we conclude that CTA [the initial transferee of the Autodesk software] was a

---

[70] Vernor v. Autodesk, Inc., 621 F.3d 1102 (9th Cir. 2010).
[71] UMG Recordings, Inc. v. Augusto, 628 F.3d 1175 (9th Cir. 2011).
[72] MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928 (9th Cir. 2010).
[73] *Vernor*, 621 F.3d at 1104-06.
[74] *Id.*
[75] *Id.*

licensee rather than an owner. . . .[76]

In *UMG*, the court refused to find that a statement on the label of an unsolicited, promotional CD delivered via mail constituted a license.[77] Even though the statements on the CDs purported to create a license, the unsolicited nature of the mailing, coupled with the lack of any affirmative statement or actions denoting acceptance made the existence of a license problematic.[78] In the absence of a license, the distribution was ruled a "first sale" immunizing the defendant from UMG's claim of copyright infringement.[79]

In *MDY*, plaintiff MDY Industries sought a declaratory judgment that sales of its software, a type of "bot" called "Glider," did not infringe Blizzard's copyright in its popular "World of Warcraft" online multi-player game.[80] Applying *Vernor*, the *MDY* court found that the End User License Agreement ("EULA"), together with the Terms of Use ("ToU"), constituted a license because Blizzard "reserves title in the software and grants players a non-exclusive, limited license. Blizzard also imposes transfer restrictions if a player seeks to transfer the license..."[81] However, the Ninth Circuit ruled that use of the Glider software, which automated play within some levels of Blizzard's game, did not infringe the online game's copyright even though it violated the ToU of the game.[82]

In coming to this conclusion, the Ninth Circuit engaged in a more detailed and nuanced[83] analysis of the exact provisions of the ToU at

---

[76] *Id.* at 1111.

[77] UMG Recordings, Inc. v. Augusto, 628 F.3d 1175, 1180 (9th Cir. 2011).

[78] *Id.* ("Our conclusion that the recipients acquired ownership of the CDs is based largely on the nature of UMG's distribution. First, the promotional CDs are dispatched to the recipients without any prior arrangement as to those particular copies. The CDs are not numbered, and no attempt is made to keep track of where particular copies are or what use is made of them. As explained in greater detail below, although UMG places written restrictions in the labels of the CDs, it has not established that the restrictions on the CDs create a license agreement.").

[79] *Id.* at 1180-81.

[80] MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 934-35 (9th Cir. 2010).

[81] *Id.* at 938.

[82] *Id.* at 941-42.

[83] *See* Nancy S. Kim, *The Software Licensing Dilemma*, 2008 B.Y.U. L. REV. 1103, 1003-04 (2008) ("[S]oftware transactions are not a binary proposition. While some transactions can clearly be identified as either licensing or sales deals, most

issue to determine whether they constituted conditions on the copyright license or were purely contractual in nature. In this context, the court stated that "contractual terms that limit a license's scope [are] 'conditions,' the breach of which constitute copyright infringement."[84] The court referred "to all other license terms as 'covenants,' the breach of which is actionable only under contract law."[85] Applying this distinction between conditions and covenants to the provisions at issue, the court determined that the prohibition on the use of automated "bots" was a covenant, rather than a condition.[86] Therefore, the use of bots in violation of the ToU was simply a breach of contract and did not rise to the level of copyright infringement.

As justification for this conclusion, the court provided the following policy views:

> Were we to hold otherwise, Blizzard—or any software copyright holder—could designate any disfavored conduct during software use as copyright infringement, by purporting to condition the license on the player's abstention from the disfavored conduct. . . . This would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners.[87]

In concluding its analysis of conditions and covenants, the Ninth Circuit held that "for a licensee's violation of a contract to constitute copyright infringement, there must be a *nexus* between the condition and the licensor's exclusive rights of copyright."[88] In other words, "the potential for infringement exists only where the licensee's action (1) exceeds the license's scope (2) in a manner that implicates one of the licensor's exclusive statutory rights."[89]

---

entail both.")

[84] *MDY*, 629 F.3d at 939.

[85] *Id*.

[86] *Id.* at 939-40.

[87] *Id.* at 941.

[88] *Id.* (emphasis added).

[89] *Id.* at 940. The *MDY* court also used the phrasing "the copyright owner's complaint must be grounded in an exclusive right of copyright" in place of "in a manner that implicates one of the licensor's exclusive statutory rights." *Id.*

Together, *Vernor, UMG,* and *MDY* show an increasing focus on the proper balance between copyright law and contract law. In particular, the policy discussion in *MDY* exhibits a firm recognition that licensing agreements present an opportunity for the misuse and unsanctioned extension of copyright rights.[90] As such, the *Vernor* court refined the legal test for distinguishing between a license and a contract for sale. Further, even after determining that the agreement contained a copyright license, the *MDY* court created an explicit test for determining whether a particular provision in a license agreement exceeds the scope of rights that Congress sought to confer upon copyright owners and therefore should be regarded solely as a contractual covenant.

The remainder of this Article applies these new legal tests to the GPL. In particular, several of the GPL's most debated terms are applied to different scenarios and interpreted in light of the *MDY* trio of cases. Under these cases, it is possible that either: 1) the GPL may be found to be a contract and not a license, or 2) the provisions of the GPL which necessitate the disclosure of non-derivative source code to downstream recipients may be construed as contractual covenants. If true, in neither case would a remedy of copyright infringement be forthcoming.

### *C. General Public License or General Public Contract?*

Arguably, the GPL is not a license agreement at all, despite its internal protestations to the contrary.[91] In *Vernor,* to qualify an agreement as a license, the court required that the copyright owner (1) specify that a user is granted a license, (2) include significant restrictions on the transfer of the software, and (3) include notable use restrictions.[92] The GPL refers to itself as a license several times and states clearly that the recipient of the software is only being granted a

---

[90] *See* Justin Van Etten, *Copyright Enforcement of Non-Copyright Terms:* MDY v. Blizzard; Krause v. Titleserv, 2011 DUKE L. & TECH. REV. 7, 42 (2011) ("The Ninth Circuit, in *MDY*, has explicitly created a rule against rightsholders using copyright to enforce non-copyright terms, and has based this rule in the unequivocal policy arguments that copyright should not be expanded by contract.").

[91] *See, e.g.*, GPL v2, Section 4.

[92] Vernor v. Autodesk, Inc., 621 F.3d 1102, 1110-11 (9th Cir. 2010).

license. Section 1 allows for copying and distribution of "verbatim copies" of the Program under several minor conditions: namely, the software must include a copyright notice, keep intact all notices that refer to the GPL, and provide any recipients of the software with a copy of the GPL.[93] Section 3 provides additional terms required in order to distribute the Program in object code. One could also view the "copyleft" requirements of Section 2 as a form of restriction on the transfer of the software in the sense that distribution of a work based on the Program is only permitted if it is also licensed under the terms of the GPL. The GPL appears to satisfy at least the first two requirements of the three-part *Vernor* test. [94]

However, the GPL does not appear to include any notable use restrictions.[95] Use of software licensed under the GPL is not restricted to the extent it does not involve distribution: "The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program)."[96] In addition, neither copying nor modification carries any additional restrictions absent subsequent distribution. Thus, while restrictions are placed upon the creation of derivative works and the distribution of copies of the work, there do not appear to be any restrictions regarding the actual "use" of the program. Absent provisions restricting use, a strict literal reading of the *Vernor* decision implies the GPL is not a license.

However, given the unique "copyleft" requirements of the GPL

---

[93] These conditions may not rise to the level of "significant" restrictions, however.

[94] One can argue, however, that copying and distribution of "verbatim *copies*" under Section 1 or 3 is not the same, in a strict legal sense, as transferring *the* licensed copy of the program. In this sense, *Vernor*'s requirement of "significant restrictions on the transfer of the software" could be interpreted to require restrictions on the particular, primary copy that is the original subject of the license. 621 F.3d at 1110-11. Furthermore, the copyleft provisions are referring to distribution of a modified work rather than transfer of the particular copy that is the primary subject of the license.

[95] *See, e.g.*, Eben Moglen, *Enforcing the GNU GPL*, FREE SOFTWARE FOUNDATION, Sept. 10, 2001, http://www.gnu.org/philosophy/enforcing-gpl.html ("The license does not require anyone to accept it in order to acquire, install, use, inspect, or even experimentally modify GPL'd software.").

[96] GPL v2, Section 0.

and the ambiguous, non-statutory nature of the term "use," a court may construe other GPL provisions as providing restrictions on use. In fact, the *Vernor* court itself noted that "the SLA [Software License Agreement] also imposed use restrictions against . . . modifying, translating, or . . . removing any proprietary marks from the software or documentation."[97] While a prohibition against modification or translation is better classified as a restriction on derivative work rights, the *Vernor* court explicitly recognized these as restrictions on "use" in fulfillment of the third requirement.[98] With this in mind, it appears likely that the GPL would be interpreted as a license under a *Vernor*-styled framework due to the restrictions discussed above.[99]

Even if the GPL is found to be a license, however, certain provisions, when scrutinized under the *MDY* test, are likely to be found to be contractual covenants rather than conditions upon the license grant.

### *D. Alternative Interpretations of the GPL Applied in Light of* MDY

#### 1. Distribution of a Loadable Kernel Module Standing Alone

The implications of the *MDY* case for GPL's applicability to loadable kernel modules are profound. As stated by the Ninth Circuit in *MDY*, a finding of copyright infringement will only follow if there is a nexus between the provision contained within the agreement and the licensor's exclusive rights of copyright.[100] Assuming loadable

---

[97] *Vernor*, 621 F.3d at 1111.

[98] In addition, Autodesk's restriction on "removing any proprietary marks from the software," *id.*, may be analogous to the GPL's requirement to maintain copyright notices and provide a copy of the license to any downstream licensee.

[99] It is also possible that a court would interpret the GPL as ineffective in light of *UMG*. Similar to the "license" denied in *UMG*, the GPL does not provide for any affirmative interaction between the putative licensor and licensee. For more discussion of whether the GPL's notice and language are sufficient to form a binding contract under traditional "offer and acceptance" doctrine, *see* Kumar, *supra* note 5, at 16-19; Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1132-33 (2000); Christian H. Nadan, *Open Source Licensing: Virus or Virtue?*, 10 TEX. INTELL. PROP. L.J. 349, 362-63 (2002).

[100] MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 941 (9th Cir.

kernel modules are not derivative works of the Linux kernel,[101] distribution of such modules under a license other than the GPL or without the corresponding source code is at worst breach of a covenant within the GPL, not meriting a finding of copyright infringement.

Under a narrow interpretation of the GPL, discussed in Section II, *supra*, a "work based upon the Program" is equivalent in scope to the concept of derivative works under the Copyright Act. If this is the case, then the requirements of the lettered conditions of Section 2 and of the collective works provision only apply to modified works that would qualify as derivative works. Assuming that loadable kernel modules containing only unprotected, functional code are not derivative works of the Linux kernel, the requirements of the GPL do not extend to these modules in any fashion. Thus, any entity that holds a copyright on the kernel would not have any claim, grounded in either contract or copyright law, that the terms of the GPL were breached or the copyright infringed.

Under the broader interpretation of the GPL discussed in Section III.A, *supra*, the term "work based on the Program" incorporates any work that contains any portion of the Program, no matter how insignificant. In this case, the lettered conditions of Section 2 and the collective works provision reach beyond a derivative works analysis and require compliance with the GPL for programs containing any portion of the code.[102] However, non-compliance with these conditions would not trigger a finding of copyright infringement because distribution of a *non-derivative* work, standing alone, does not implicate, or have a nexus with, any of the copyright holder's exclusive rights any more than distribution of a completely unrelated work does.[103] Thus, under an *MDY* analysis, even the broader reading of the GPL results only in a breach of contract action for distribution

---

2010).

[101] *See supra* Section II.B.

[102] This is assuming that the plaintiff copyright holder would be able to satisfy a preliminary showing that a contract was, in fact, formed under Section 5 of the GPL.

[103] *See, e.g.*, Nadan, *supra* note 99, at 369 ("The copyleft provision [of the GPL] purports to infect independent, separate works that are not derivative [works] . . . . Attempting to extract such rights exceeds the scope of the copyright.").

of a loadable kernel module that is not a derivative work. The implications of this finding regarding availability of remedies are discussed in Section III.E, *infra*.

2. Distribution of a Loadable Kernel Module in Conjunction with an Unmodified Linux Kernel

Adding an unmodified Linux kernel into the distribution package should not change the legal conclusions reached above. Under the narrower interpretation of the GPL, the loadable kernel module is not a derivative work for the reasons set forth in Section II.B, *supra*, and the requirements of the GPL only extend to the unmodified kernel. Thus, the developer may distribute the unmodified kernel in full compliance with Section 1 of the GPL and distribute the module as he sees fit. Because neither the unmodified kernel nor the module is a derivative work, the terms of Section 2 are never triggered or implicated. Thus, under an interpretation of the GPL that hinges upon a derivative works analysis, any entity that holds a copyright on the kernel would not have any claim, grounded in either contract or copyright law, that the terms of the GPL were breached or the copyright infringed by the distribution of a loadable kernel module and an unmodified kernel.

Under the broader interpretation of the GPL, in which a "work based on the Program" includes any program containing any portion of the kernel code, the module is subject to the requirements of the lettered conditions of Section 2 and the collective work provision. However, non-compliance with these requirements still amounts to only a breach of contact claim. This is because the breach of contract claim could only be based upon failure to distribute the module in compliance with the requirements of Section 2; the unmodified kernel is in complete compliance with the distribution requirements of Section 1.[104] As discussed above in Section III.D.1, if the module is not a derivative work but still subject to the terms of the GPL, then non-compliance with the GPL will only lead to a breach of contract claim: Distribution of an independent, non-derivative work does not

[104] This analysis does not apply however, if the unmodified kernel and the module are, together, considered a single "modified work as a whole" or a collective work. *See* Section III.D.3, *infra*.

implicate, or have a nexus to, any of the copyright holder's exclusive rights. Thus, under the broader interpretation of the GPL, distribution of a loadable kernel module with an unmodified version of the Linux kernel still only exposes the distributor to a possible breach of contract claim.

3. Distribution of a Loadable Kernel Module in Conjunction with a Modified Linux Kernel

The legal results reached in the two preceding scenarios are drastically altered if the distributor chooses to also distribute a *modified* version of the Linux kernel. Under the narrower interpretation of the GPL, although the module would not qualify as either a derivative work or a "work based on the Program," the modified kernel would qualify as both. With this in mind, the requirements of the lettered conditions of Section 2 and the collective works provision would apply to the modified kernel. The legal conclusion to this scenario depends upon a reading of the collective works provision. In particular, whether the loadable kernel module and the modified Linux kernel, when distributed together, constitute a "modified work as a whole" or collective work will determine whether the result is a copyright infringement or simply a breach of contract claim.[105]

If the two programs, when distributed together, are ruled to constitute a "modified work as a whole," then the copyright has been infringed because the modified kernel is unquestionably a derivative work of the original kernel. Therefore, a provision that restricts how this derivative work may be distributed would have nexus to the exclusive distribution right of the copyright holder. As such, non-compliance with this provision would lead to a finding of copyright infringement.

If the modified kernel and the loadable module are *not* found to be a single "modified work as a whole," then the GPL has been complied with if distribution of the modified kernel accords with all

---

[105] For the Free Software Foundation's interpretation of the phrase "modified work as a whole," *see Frequently Asked Questions About Version 2 of the GNU GPL*, FREE SOFTWARE FOUNDATION, http://www.gnu.org/licenses/old-licenses/gpl-2.0-faq.html#MereAggregation (last updated Jan. 8, 2012).

requirements of Section 2, regardless of whether the source code of the module is opened. Under the narrower interpretation of the GPL, a loadable kernel module that is not a derivative work does not implicate any provisions of the GPL because it is not a "work based on the Program." As long as the modified kernel is distributed in accordance with the GPL, the module is not implicated and there is no claim grounded in either contract or copyright law.

Analysis similar to the above also applies under the broader interpretation of the GPL, in which the copyleft requirements apply to both the module and the kernel. If the module and the kernel are ruled to be a single "modified work as a whole," then failure to provide source code for the module would likely be ruled a copyright infringement because the modified kernel is a derivative work. If the module is considered to be part of a single work with the kernel, then it too would be a derivative work and a provision regarding distribution of this derivative work would have a nexus to the copyright holder's exclusive distribution rights.

However, if the loadable module is *not* considered part of the "modified work as a whole" then failure to provide source code for the module would only give rise to a breach of contract claim. Operating under the broader interpretation of the GPL, all copyleft provisions apply to the module, regardless of whether it is a derivative work. However, because it is *not* a derivative work, distribution of this non-derivative work would not implicate, or have a nexus to, any of the copyright holder's exclusive rights, and thus noncompliance would amount solely to a breach of contract.

### *E.* MDY*'s Effect on Availability of Remedies for Non-Compliance with the GPL*

Absent a finding of copyright infringement, the plaintiff's remedies must flow from a breach of contract claim. As the court in *MDY* implied, breach of contract remedies are generally confined to damages, and those damages are "generally limited to the value of the actual loss caused by the breach."[106] On the other hand, the remedies

---

[106] MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 941 n.3 (9th Cir. 2010). *See also*, Sean Hogle, *Conditions vs. Covenants: California Rulings Threaten the Practical Enforceability of Open Source Licenses*, 25.9 COMPUTER &

available to a copyright holder following a successful infringement claim are much more favorable and include lost profits or a reasonable royalty, statutory damages of as much as $150,000 (regardless of actual damages), and attorney's fees in exceptional cases.[107]

In a case where the GPL itself mandates that source code be provided for free,[108] damages for breach will be very difficult, if not impossible to ascertain, and arguably zero.[109] Unlike the situation in which a case is brought under copyright law, injunctive relief in a breach of contract case is rarely awarded, especially when it is not stipulated to within the agreement itself.[110] The GPL contains no such reference to injunctive relief as a remedy for violation of its provisions. Thus, "in the open source context, where software is licensed without charge, establishing economic loss could prove daunting if not impossible."[111] As such, even if a plaintiff is victorious on the merits of a breach of contract claim based upon non-compliance with the GPL, he may be unable to fashion any practical remedy.

---

INTERNET LAW. 1, 2 (2008) [hereinafter Hogle, *Conditions*]; *but see* Jose J. Gonzalez de Alaiza Cardona, *Open Source, Free Software, and Contractual Issues*, 15 TEX. INTELL. PROP. L.J. 157, 187 (2007) ("If [the GPL] is a contract, it seems that a person who refuses to comply with the terms of the GNU GPL could be forced to release the source code of his derivative work."). Dr. Gonzalez is presumably arguing that this forced "opening" could be reached under a specific performance doctrine.

[107] Hogle, *supra* note 106, *Conditions* at 2; Van Etten, *supra* note 90, at 11 (2011).

[108] GPL v2, Section 1.

[109] Kumar, *supra* note 5, at 15 ("If [contractual] consideration for the author is the release of changes back to the community, how would a court financially compensate the author under contract law? Money damages would not be an appropriate remedy . . . .").

[110] Hogle, *supra* note 106, *Conditions* at 2 ("[I]njunctive relief is facilitated by the irreparable harm presumption that applies if the plaintiff is likely to succeed on the merits of the copyright infringement claim. . . . [while i]njunctive relief is typically not available for breach of contract claim."

[111] *Id.*

## CONCLUSION

Linux is a very popular operating system that is increasingly used in embedded devices. Uncertainty regarding the legal consequences of modifying proprietary software for, or simply linking proprietary software to, a device running the Linux kernel makes it difficult for developers of the proprietary software and embedded devices to reach agreement.

The reason for uncertainty is the GPL, the license to which all those using, modifying, or distributing Linux are bound. The GPL purports to require that any software derived from or linked to software licensed under it be distributed for free, with all source code included. Requiring developers to distribute proprietary software for free removes their ability to be compensated for providing their code to a third party in object form. Requiring distribution of the corresponding source code is even more damaging, because publication of the source releases trade secrets to not only the version of the code distributed under the GPL (say for a Linux version), but for the same version released under a proprietary license (e.g., for any other operating system).

Assuming Linux kernel modules only contain the source code or headers necessary to enable efficient interoperability of proprietary code with the Linux kernel, the modules fall squarely within the analysis articulated by *Altai*, *Accolade*, and *Connectix* for successful avoidance of classification as a derivative work. For the GPL to reach beyond derivative works of the Linux kernel and effectively require any software linked to it be distributed for free and with software's source code: (1) the GPL must be interpreted as a license rather than a contract, and (2) the provisions of the license which are breached must be of a type such that their breach merits a finding of copyright infringement.

According to the recent Ninth Circuit *MDY* holding, a finding of copyright infringement will only follow if there is a nexus between the conditions (of the license) and the licensor's exclusive rights of copyright. Unless the "licensee's" software is determined to be a derivative work of software licensed under the GPL, none of the exclusive rights of copyright are implicated, because though reproduction and distribution occur, they are not reproduction or distribution of anything in which the copyright holder has a legal

interest. In essence, the recent *MDY* ruling, together with conventional derivative works analysis, makes software modules linked to the Linux kernel freely licensable without regard to release of those modules' source code because there is no practical remedy for a licensee's failure to follow the terms of the GPL.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 3 WINTER 2012

# ESSAY

## INTERNET AS A HUMAN RIGHT: A PRACTICAL LEGAL FRAMEWORK TO ADDRESS THE UNIQUE NATURE OF THE MEDIUM AND TO PROMOTE DEVELOPMENT

*Young Joon Lim and Sarah E. Sexton*[*]


Cite as: 7 Wash J.L. Tech. & Arts 295 (2012)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1114

ABSTRACT

*A Taiwanese court sentenced a blogger to 30 days of detention for her comments that a restaurant's food was too salty and that the locale was unsanitary. In Indonesia, a woman was sentenced to six months in jail for libel after an e-mail she sent to friends about poor treatment she received in a hospital was posted on Facebook. These are not isolated cases of persecution, but part of a broad pattern of challenges facing individuals around the world. The United Nations recently released a report on legal trends involving restriction of expression on the Internet, declaring that freedom of expression on the Internet is a human right. If Internet freedom is a human right, what are the limits of that entitlement? This Essay explores existing legal models and restrictions on online communication through case studies, including discussion of restrictions in countries affected by the Arab Spring of 2011. This Essay suggests six basic elements for a legal framework that can support the unique challenges presented by the Internet as it becomes a primary mode of communication.*

---

[*] Sarah E. Sexton, UC Berkeley, School of Law (Boalt Hall), Class of 2010. Young Joon Lim, Ohio University, E.W. Scripps School of Journalism, Ph.D. Candidate 2013. Thank you to our families, Dr. Michael Sweeney, and Alicia Hoffer for her assistance with this publication.

TABLE OF CONTENTS



## INTRODUCTION

The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, recently released a report on the trends and challenges facing

freedom of expression, with particular concentration on the Internet.[1] The report received a great deal of press attention and was greeted with headlines such as, "The U.N. Declares Internet Access a Human Right."[2] Some articles have questioned the notion of Internet access as a human right, and the headlines raise the question of whether access to and freedom of expression on the Internet are deserving of the same respect as other human rights. What is the place of such rights in existing legal systems? What legal framework can be used to protect such rights on the Internet, a milieu that is often thought of as wild, borderless, and anonymous?

The Internet and other new telecommunications technologies affect many facets of society, and bring with them the opportunity to generate disagreements and discord. As such, societies need a way to resolve these disputes while protecting the interests of the parties involved. A legal framework can help maintain order and bring resolution to conflicts. It is necessary for such a legal framework to address the unique challenges presented by the Internet as it becomes a primary mode of communication.

Across the globe, different approaches are emerging. Certain regimes have adopted approaches that infringe on their citizens' basic human rights. Restrictions on Internet access and online expression limit many of the freedoms considered to be basic human rights, as recognized by international bodies such as the United Nations. To bring greater legitimacy to the rights of citizens to access the Internet and freely post online, a legal framework recognizing access to the Internet and freedom of expression online as human rights should be adopted.

This Essay explores the treatment of Internet freedom as a human right and considers the limits to that entitlement. It considers existing legal models and restrictions on online communication and access.

---

[1] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, delivered to General Assembly*, U.N. Doc. A/HRC/17/27 (May 16, 2011) [hereinafter *Report of the Special Reporter*].

[2] Adam Clark Estes, *The U.N. Declares Internet Access as a Human Right*, ATLANTIC WIRE (June 6, 2011), http://www.theatlanticwire.com/technology/2011/06/united-nations-wikileaks-internet-human-rights/38526.

The analysis focuses on protecting freedoms.

## I. WHY DOES INTERNET FREEDOM MATTER?

To some, the Internet may seem like a modern luxury, and the suggestion that Internet access should be considered a human right may seem exaggerated. This criticism might ring true if the right were an entitlement—if Internet access as a human right meant that governments should issue laptops to citizens and provide wireless connections. More realistically, access to the Internet and freedom of expression, opinion, and speech online are simply contemporary technological manifestations of the existing human right of freedom of expression, opinion, and speech as recognized by the International Covenant on Civil and Political Rights.[3] As technology adapts and presents new modes of communication, new forums for expression flourish. Because these rights are inherently tied to human and economic development, freedom of expression online and access to the Internet deserve international attention and global, cooperative enforcement.

It is important to recognize that rights and development are intertwined in a way that is simultaneous and codependent. Here, whether recognition of expression rights fosters development, or whether development is itself exertion of rights, is beyond the scope of this analysis. The Internet has proven an effective tool for the promotion and protection of human rights by disseminating information.[4] It is an enabler of other economic, social and cultural, as well as civil and political, rights.[5]

The Internet's speed also facilitates rapid action to respond to human rights violations and may supply accurate, real-time information. Human rights organizations are able to use the Internet in their operations in innovative ways. Also, the Internet serves as a

---

[3] International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), 21 U.N. GAOR, 21st Sess., Supp. No. 16 at 52, U.N. Doc. A/6316 (Dec. 16, 1966), *available at* http://www2.ohchr.org/english/law/ccpr.htm [hereinafter Covenant on Civil and Political Rights].

[4] HUMAN RIGHTS AND THE INTERNET 7 (Steven Hick, Edward F. Halpin, & Eric Hoskins eds., 2000).

[5] *See Report of the Special Reporter*, *supra* note 1, at 7.

means to educate, organize and track information about human rights violations.[6] An example of the Internet's ability to quickly disseminate on-the-ground information is the way postings from Tunisians' Facebook pages during the revolution of 2011 were collected, translated, and reposted on the website Nawaat, an independent blog produced by Tunisians in exile.[7] The information then passed via Twitter to mainstream journalists.[8]

Furthermore, access to information and a free press increase transparency, reduce corruption, stir debate, and keep pressure on governments. The Internet is a means of gaining broader political participation, and it sparks dialog to influence government and the democratic process.[9] As a medium, the Internet is unique in making it easier for a broader range of voices to access information without the influence of institutions or entrenched power-holders. Citizen journalists spread their messages and their realities through the eyes of those on the ground. Bloggers and online forums offer alternative sources of information. Governments are less able to control the flow of information than through traditional media.[10]

The borderless nature of the Internet is an international exchange point. Movements can be trans-nationalized and build support from and solidarity with individuals across the globe.[11] During the Arab Spring uprisings in early 2011, for example, the governments of China and Iran attempted to block the flow of images and information of the uprisings on their news networks and Internet.[12] In China, the reaction was strong because the government feared a "Jasmine

---

[6] Lloyd Axworthy, *The Mouse is Mightier than the Sword*, *in* HUMAN RIGHTS AND THE INTERNET 16, 19 (Steven Hick, Edward F. Halpin, & Eric Hoskins eds., 2000).

[7] JEFFREY GHANNAM, SOCIAL MEDIA IN THE ARAB WORLD: LEADING UP TO THE UPRISINGS OF 2011 16 (2011), *available at* http://cima.ned.org/sites/default/files/CIMA-Arab_Social_Media-Report%20-%2010-25-11.pdf.

[8] *Id.*

[9] Bruce Etling, Robert Faris & John Palfrey, *Political Change in the Digital Age: The Fragility and Promise of Online Organizing*, 30 SAIS REV. 37 (Summer-Fall 2010), *available at* http://dash.harvard.edu/handle/1/4609956.

[10] *Id.*

[11] Simon Cottle, *Media and the Arab Uprisings of 2011: Research Notes*, 12 JOURNALISM 647, 654 (2011), *available at* http://www.contexting.me/files/CottleMediaandtheArabUprising.pdf.

[12] *Id.* at 655.

Revolution" modeled on the pro-democracy protests that were spreading across the Arab world.[13]

The decentralized associations and loose networks formed through the Internet just described enable change in authoritarian regimes.[14] Yet such regimes are simultaneously becoming more sophisticated in blocking, tracking, and limiting Internet access and online expression. States have begun to monitor and filter online content and posters, including through cyber-attacks, threats, and intimidation. Governments also have employed the law as a means to control online speech.[15] China and Iran stand out as the most egregious in their control of online information. Still, several dozen countries filter the Internet, such as Burma, Tunisia, Uzbekistan, and Vietnam.[16]

## II. EXISTING FRAMEWORK

### *A. Legitimate Restrictions*

While the freedoms of speech, expression, and opinion are well-recognized among the international community, even absolutists recognize that there are appropriate boundaries to these freedoms. For example, certain types of expression are restricted to promote public safety and the interests of society. Examples of restricted speech include child pornography; hate speech; direct and public incitement to commit genocide; and advocacy of national, racial, or religious hatred that constitutes incitement to discrimination or violence.[17] While some restrictions are absolute and serve to protect the rights of individuals, such as the right to life,[18] a gray area emerges surrounding legal concepts such as defamation. Different cultures take varying approaches as to how to distinguish between legitimate and restricted expression. The following sections describe some of the existing structures.

---

[13] *Id.*
[14] Etling, Faris & Palfrey, *supra* note 9.
[15] *Id.*
[16] *Id.*
[17] *See Report of the Special Reporter*, *supra* note 1, at 8.
[18] *Id.*

### *B. Article 19*

Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, as adopted by the General Assembly of the United Nations, provides that everyone has the right to express his or herself through any media.[19] Article 19 guarantees that every person has the right to hold opinions without interference and to freedom of expression, including freedom to seek, receive, and impart information and ideas of all kinds. Notwithstanding, Article 19 includes limits aimed at protecting national security, public order, public health, morals, and the rights and reputations of others.[20]

The U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression interprets Article 19 to be so inclusive as to adapt to any modern technological development. The broad language of the article was drafted with the foresight to accommodate the Internet and the burst of new modes of media.[21]

### *C. Comment 34*

In July 2011, the United Nations Human Rights Committee adopted General Comment 34 to Article 19, suggesting that freedom of opinion and of expression are "indispensable conditions for the full development of the person."[22] The comment further states that these freedoms are essential for any society. Freedom of expression is necessary for government transparency and accountability, two elements essential for the promotion and protection of human rights. General Comment 34 specifically states that means of expression include the Internet and all forms of audio-visual and electronic and

---

[19] Covenant on Civil and Political Rights, *supra* note 3.

[20] Mark Erik Hecht & Rodney Neufeld, *The Internet and International Children's Rights*, *in* HUMAN RIGHTS AND THE INTERNET 153-54 (Steven Hick, Edward F. Halpin, & Eric Hoskins eds., 2000).

[21] *See Report of the Special Reporter*, *supra* note 1.

[22] Human Rights Committee, *General Comment No. 34, Article 19: Freedoms of Opinion and Expression*, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011).

Internet-based modes of expression.[23] The comment emphasizes that states should take into account developments in technologies and how communications have changed as a result. Comment 34 encourages states to foster the independence of new media and to ensure access to them.

Comment 34 does not advocate unfettered discretion for the restriction of freedom of expression; it suggests that laws must guide authorities as to what type of expression may be properly restricted. Specifically, Comment 34 supports the restriction of freedom of expression in order to protect other rights. Restrictions "on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines" are only permissible to the extent that they are compatible with promoting human rights, transparency, and accountability. Comment 34 also condemns prohibiting the publication of material solely on the basis that it may be critical of a government or political system.

Comment 34 also addresses defamation, the treatment of which has been a point of contention in regulation of speech. The comment advocates for the precise tailoring of defamation laws to ensure that they comply with the principles of transparency and accountability, suggesting the decriminalization of defamation. Laws that criminalize defamation should leave room for defenses of truth and not be applied to "those forms of expressions that are not, of their nature, subject to verification."[24] Comment 34 also suggests a greater amount of leeway with respect to public figures when the published statements are untrue but published without malice. The Comment states that imprisonment is never an appropriate punishment for defamation.

## III. EXISTING EXAMPLES OF GOVERNMENT TREATMENT OF THE INTERNET

National governments allow varying degrees of Internet freedom

---

[23] *Id.*
[24] *Id.*

and take different approaches to policing online expression. Section A discusses restrictions on Internet expression imposed by authoritarian regimes in the Middle East. Section B discusses criminalization of Internet speech in various countries. Section C describes attempts to regulate online expression through private intermediaries. Section D discusses attempts in the U.S. to restrict online speech.

### *A. Restrictions on Access and Criminalization of Content*

Governments have used blocking or filtering technologies to limit access to specific websites or to completely halt access to the Internet in order to quash undesired communications. These restrictive actions may legitimately be used to target undesired information, yet there is danger that blocking can be administered in arbitrary, secretive, and excessive ways.[25] This impedes the freedom of expression as set out in Article 19, paragraph 3 of the International Covenant on Civil and Political Rights.[26] As blocking stops more than the targeted information, its broad application is over-inclusive. Lastly, blocking is often done without the possibility for judicial review or independent monitoring.[27]

Blocking garnered international attention during the Arab Spring, during which challenged governments shut down Internet access in attempts to stop organizers and other protestors from spreading their message, rallying support, and planning their strategy online. While it is too early to comment on the effect these uprisings have wrought on domestic Internet policies, we can reflect on the systems that were in place in these countries at the time of the uprisings.

The governments, challenged by the uprisings, tried to censor and contain the dispersal of images and information by cutting the cord on the Internet, in addition to monitoring telecommunications and limiting the entry and mobility of foreign journalists. Repressive regimes deploy sophisticated digital censorship and monitoring capabilities, and they sometimes engage in cyber attacks against

---

[25] *See Report of the Special Reporter*, *supra* note 1, at 10.
[26] Covenant on Civil and Political Rights, *supra* note 3.
[27] *See Report of the Special Reporter*, *supra* note 1, at 10.

dissidents.[28] For example, in April 2008 the Egyptian government quashed a group of online organizers attempting to carry out a strike against the government by tracking them down via their digital footprints. A video of one such organizer's tearful release was widely-viewed on YouTube, and served as a powerful tool of repression.[29]

1. Egypt

In Egypt, prior to the overthrow of Mubarak in 2011, politically sensitive websites were blocked. While no law specifically gave the government power to filter such websites, the Penal Code and the Emergency Law provided the government with the authority to restrict and monitor communications.[30] Egypt's Emergency Law allowed authorities to detain individuals for long periods of time without a hearing. Egypt also relied on extralegal enforcement. It allowed censorship, indiscriminate confiscation, and forced closures as the Ministry of Interior saw fit.[31] Freedom of the press and freedom of expression faced severe limits. Egypt's Press Law criminalized criticizing the president or the leaders of foreign countries and spreading false news.[32] This law also applied to online communications. Online writers and bloggers were harassed and detained for their online and offline activities.[33] For example, in 2003 state officials detained activist Ashraf Ibrahin on charges of "spreading false news" for e-mailing stories and photographs of police violence at anti-war demonstrations to international human rights organizations.[34]

While the Mubarak government did not support unlimited access to content, it recognized the importance of access to the Internet. The Egyptian government implemented programs to expand Web access.

---

[28] *See* EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM (2011).

[29] Etling, Faris & Palfrey, *supra* note 9, at 37-49.

[30] ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 276 (Ronald Deibert et al., eds. 2008) [hereafter ACCESS DENIED].

[31] *Id*.

[32] *Id*.

[33] *Id*. at 278.

[34] *Id*.

The government started the Free Internet Program, which allowed users to access the Internet for the price of a local telephone call. This program served as a model for other developing countries. Egypt grew to have the largest fixed-line communications network in the Arab world.[35] Many Egyptian Internet users do not have personal computers but rely on Internet cafés. Internet café owners were required to obtain a license from the Ministry of Telecommunications to operate. Internet café owners also reported that security officials instructed them to keep lists of their customers and the customers' identification numbers. With four licensed Internet carriers, eight data service providers, and hundreds of Internet service providers, it is ironic that the same government which promoted this access was the same government brought down by the many people who expressed their opinions and organized online.

It is not clear what has changed following the end of the Mubarak government. The same week Mubarak was arrested, blogger Maikel Nabil was sentenced to three years in prison for "insulting the military."[36] Also, the Supreme Council issued a letter to Egyptian editors ordering them not to report on the armed forces without advanced permission. The head of the Armed Forces Morale Affairs Department, General Ismail Etman, stated at a news conference, "Freedom of expression is guaranteed as long as it is respectful and doesn't question the armed forces."[37]

The bloggers and online writers in Egypt still straddle the line between political activists and citizen journalists, speaking to topics that mainstream journalists cannot touch. These writers serve as an alternative source for information to audiences that distrust the mainstream media because of the legacy of governmental control.

2. Libya

The Libyan government systematically blocked and restricted access to the Internet. In particular, the government targeted political opposition, content critical of the government, and websites that

---

[35] *Id.* at 277.

[36] Lawrence Pintak, *Breathing Room: Toward a New Arab Media*, COLUM. JOURNALISM REV., May/June 2011, at 23.

[37] *Id.*

advocate the rights of the minority group Amazigh (Berbers).[38] The country's press laws established many restrictions, punishable by large fines and imprisonment, and made private media illegal. The laws have also been applied to expression on the Internet. Anyone convicted of disseminating information that conflicted with the constitution or "fundamental social structures," or that tarnished Libya's image abroad, could be punished with life imprisonment or even death under Libya's penal code.[39] Also, in order to obtain a ".ly" domain name, Libya's top-level domain, a website "must not contain obscene, scandalous, indecent, or contrary to Libyan law or Islamic morality words, phrases or abbreviations."[40]

3. Syria

The Syrian government has relied on vague and overly broad laws to attack various types of information. The government blocks pornographic websites and censors websites with "pro-Israel or hyper-Islamist" bents and those calling for autonomy for Syrian Kurds.[41] Syria's government maintains regulatory control over Internet service providers ("ISPs"). Internet café owners must obtain a license from the Telecommunications Department's local office and must follow the Conditions Manual, which includes specifications on the spacing between computers.

Syria's constitution protects "the right to freely and openly express his views in words, in writing, and through all other means of expression" and "the freedom of the press, of printing, and publication in accordance with the law." However, other legislative provisions allow the government to restrict these rights. For example, Article 4(b) of the 1963 Emergency Law authorizes the government to monitor all publications and communications and to arrest anyone whose crimes constitute "an overall hazard."[42] Moreover, the Press Law of 2001 gives the government control and censorship of all print media. This same law penalizes the printing of falsehoods or

[38] ACCESS DENIED, *supra* note 30, at 276.
[39] *Id.* at 321.
[40] *Id*. at 323.
[41] *Id*. at 380.
[42] *Id*. at 382.

fabricated reports and writing on topics relevant to "national security or national unity" is forbidden. The government applies these laws to online publications as well.[43] The government has prosecuted individuals for e-mailing photos or articles produced by another political party, posting information exposing police crackdowns, and voicing opposition to the government. These actions have created fear, which also leads to self-censorship.

4. Tunisia

The Tunisian government deployed a system of laws, regulations, and surveillance to keep tight control over the Internet. ISPs were required to send the Ministry of Telecommunications a list of their subscribers each month.[44] Also, ISPs, Web page owners, and Web server owners were responsible for policing the content of the pages and servers they hosted.[45] They had to ensure that content adhered to the Press Code's rules. In particular, the content could not upset public order.[46] All fixed-line Internet traffic passed through facilities controlled by the Tunisian Internet Agency, an entity established by the Ministry of Telecommunications charged with regulating the Internet and domain name system.[47] The government loads SmartFilter software onto the agency's servers and may filter content across the country's ISPs.[48]

### *B. Criminalization of Online Expression and Defamation*

Some states have gone so far as to criminalize online expression even when it is legitimate (*i.e.*, not falling into the protected categories discussed above in Section II(A)). Some governments have applied existing criminal laws to online expression, while others have enacted new laws designed for online expression.[49] These laws are

---

[43] *Id.* at 382.
[44] *Id.* at 397.
[45] *Id.*
[46] *Id.* at 398.
[47] *Id.* at 395.
[48] *Id.* at 397.
[49] *See Report of the Special Reporter*, *supra* note 1, at 10.

premised on the basis of protecting reputation and national security and on countering terrorism. In practice, they allow governments to censor and stifle dissent.[50]

Reporters Without Borders reported that in early 2012, 153 people were imprisoned on charges related to the content of their online postings.[51] The countries with the most imprisoned bloggers were China (68 prisoners), Iran (20), and Vietnam (18).[52]

The Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression disapproves of imprisonment as a punishment, arguing it is a disproportionate response to imparting information. Instead, it advocates for the decriminalization of defamation. Defamation is a communication that tends to damage another's reputation. It includes any publication that exposes a person to distrust, hatred, contempt, ridicule, or anything that may impute incompetence, incapacity, or unfitness in the performance of an individual's trade, occupation, or profession.[53] The report further instructs that criminal protections in the name of national security or counter-terrorism should be limited to situations in which the government can demonstrate that: "(a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence."[54]

As forums to express one's opinion about businesses, services, and government are becoming increasingly prevalent on the Internet, people describe their unfortunate experiences or post harsh reviews of poor customer service. But there are more opportunities for the recipients of reviews to react.

For example, a simple statement ("The beef noodles were too salty") posted on a review website may have been an honest reaction

---

[50] *Id.*

[51] Reporters Without Borders, *Press Freedom Barometer 2012*, http://en.rsf.org/press-freedom-barometer-netizens-imprisoned.html?annee=2012 (last visited Feb. 11, 2012).

[52] *Id*.

[53] GEORGE L. BLUM, CRITICISM OR DISPARAGEMENT OF DENTIST'S CHARACTER, COMPETENCE, OR CONDUCT AS DEFAMATION, 120 A.L.R. 5TH 512 (2004).

[54] *See Report of the Special Reporter*, *supra* note 1, at 11.

to a less-than-stellar meal, but it also amounted to an arrestable offense in Taiwan. In June of 2011, The Taichung branch of the Taiwan High Court sentenced Taiwanese blogger Liu to 30 days in detention, suspension for two years, and a fine of 200,000 New Taiwan Dollars payable to the restaurant that received the below-average review. Liu wrote that the restaurant's food was too salty and that the locale was unsanitary and infested with cockroaches. She also criticized the way the owner let customers park their cars. The restaurant owner filed charges against her and accused her of defamation. The Taichung District Court ruled that the blog post exceeded reasonable bounds. While the court found that her comment about the cockroaches was narration of facts and not intentional slander, it found that the comments about unsanitary conditions were untrue based on health inspector reports.[55]

In Indonesia, Prita Mulyasari was sentenced to six months in jail for libel after she emailed her friends about the poor treatment she received at the Omni International Hospital. When the hospital misdiagnosed her with dengue fever, she e-mailed 20 of her friends about her experience. The friends then posted her criticism of the hospital on their Facebook pages without her knowledge. The hospital pursued criminal and civil cases against Mulyasari. Initially, the courts rejected both cases, but prosecutors appealed. The Supreme Court convicted Mulyasari of libel under the Electronic Information and Transactions Law. While the law allows for six years in jail as punishment, Mulyasari received a suspended six-month jail term.[56]

These are not isolated cases, but part of a broader challenge facing individuals around the world. Criminalization of defamation remains a hotly contested topic at the international level.

### *C. Intermediary Enforcement*

Because the Internet depends largely on private companies to provide access, connectivity, hosting, and online forums, ensuring

---

[55] Lin Liang-che, *Blogger Given Suspended Prison Sentence Over Critical Restaurant Review*, TAIPEI TIMES (Jun. 23, 2011), http://www.taipeitimes.com/News/taiwan/archives/2011/06/23/2003506487.

[56] *Indonesia Woman Gets Suspended Term for Facebook Libel*, BBC NEWS (Jul. 11, 2011), http://www.bbc.co.uk/news/world-asia-pacific-14104471.

freedom of online expression poses additional challenges. ISPs and online platforms have enjoyed relative immunity from liability for third-party content communicated via their services. However, some governments have begun to recognize these intermediaries as a more easily-reached link in controlling communications. As a result, legal protections for these intermediaries are eroding.[57] Countries may call upon ISPs to cut service to individuals or larger populations. They may also try to hold companies accountable for content posted by third-parties on their websites. For example, the European Union has a policy of notice and takedown that protects the intermediary.[58] The process is not transparent, and it is executed by the private company.

Intermediary enforcement is inherently problematic in a capitalist marketplace. A neutral body is needed to enforce the rules and ensure a level playing field. The U.N. Special Rapporteur suggests that intermediaries should: only enforce restrictions after judicial intervention; be transparent to users or the wider public about the measures they take; and, if possible, warn users before the implementation of restrictive measures.[59] Most importantly, La Rue suggests intermediaries limit their enforcement to the content at issue. As a parallel, users should have a means of appealing any enforcement action.[60]

The public-forum doctrine has emerged in response to these concerns. This doctrine recognizes that speech should be protected online but that not all online speech is the same. The case law creates three categories: (1) traditional public forums, (2) designated public forums, and (3) nonpublic forums. Regulation of speech within nonpublic forums is not subject to the same level of scrutiny as speech in public forums.[61] As mentioned above, the vast majority of online forums rely on a privately owned company. The private company regulates content. This creates an Internet with virtually no public spaces.[62] Thus, the level of scrutiny applied to restrictions of

---

[57] *See Report of the Special Reporter*, *supra* note 1, at 11.

[58] *Id*.

[59] *Id.* at 14.

[60] *Id*. at 21.

[61] DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE 71 (2009).

[62] *Id*. at 77.

Internet speech is low.

In the United States, the law generally protects ISPs and websites from liability for content passed through their services. Section 230 of the Communication Decency Act (CDA) of 1996 provides immunity from liability to ISP's that publish information offered by third parties.[63] Under Section 230, it is usually difficult to hold ISPs accountable, but this norm is not without exception. Recent cases involving MySpace and Craigslist indicate courts may be amenable to the idea of holding websites accountable for actions resulting from information they transmit.[64] In *Doe v. MySpace*, the Fifth Circuit affirmed the district court's ruling that Section 230's "Good Samaritan" provision barred the plaintiff's negligence action against MySpace for failure to protect her underage daughter from a predator she met on the social networking site.[65]

In *Doe IX v. MySpace*, the district court in Texas granted a motion to dismiss a suit brought by the parent of a child who was assaulted by a sexual predator the child met on MySpace.[66] There, the court, unlike the Fifth Circuit, considered and found that MySpace was partially responsible for creating information exchanged.

In *Chicago Lawyers' Committee For Civil Rights Under Law, Inc. v. Craigslist, Inc.*, the Seventh Circuit held that Craigslist had not violated the Fair Housing Act by allowing rental advertisements that stated preference with respect to race, religion, sex, or family status.[67] While the court ruled in favor of Craigslist yet again under the protections of Section 230, it noted that Section 230 immunity does not apply to online service providers when they "materially contribute" to the unlawfulness of the content.[68] As the Ninth Circuit explained in *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, "the Communications Decency Act was not meant to create a lawless no-man's-land on the Internet."[69]

---

[63] 47 U.S.C. § 230 (2006).

[64] *See* Shahrzad Radbod, *Craigslist—A Case for Criminal Liability for Online Service Providers?*, 25 BERKELEY TECH. L.J. 1 (2010).

[65] Doe v. MySpace, 528 F.3d 413 (5th Cir. 2008).

[66] Doe IX v. MySpace, 629 F.Supp. 2d 663 (E.D. Tex. 2009).

[67] Chicago Lawyers' Comm. For Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008).

[68] *Id*.

[69] Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521

Most recently, in August of 2011, the Internet company Google entered into a settlement agreement in which it forfeited $500 million to the United States Department of Justice after it was targeted for content advertised through its online AdWords program. Google sold ads through AdWords to Canadian pharmacies advertising drugs to U.S. audiences. Google agreed to pay a $500 million settlement.[70] This amount represents the estimated revenue the Canadian pharmacies received from their sales to the United States consumers. Google was aware that the Canadian pharmacies were illegally shipping prescription drugs into the United States. Google blocked other countries' pharmacies from doing the same but continued to sell advertisements to the Canadian pharmacies. In 2009, Google stopped these sales when it became aware of the government's investigation.[71] In the agreement, Google acknowledges improperly assisting Canadian online pharmacy advertisers in running advertisements that targeted a U.S. audience.[72] The government stated that it would hold companies accountable for violating "federal law and put[ting] at risk the health and safety of American consumers."[73] At this point, it is unclear how far this reach will extend to Internet companies.

The lesson gleaned from the above cases involving Craigslist, MySpace, and Google is that even in the United States the government puts pressure on private Internet companies to police third-party content communicated via their websites. This responsibility places an added burden on companies and serves as a hurdle to emerging Web-based businesses.

---

F.3d 1157, 1164 (9th Cir. 2008).

[70] Press Release, Department of Justice, Google Forfeits $500 Million Generated by Online Ads & Prescription Drug Sales by Canadian Online Pharmacies (Aug. 24, 2011), http://www.justice.gov/opa/pr/2011/August/11-dag-1078.html.

[71] David Goldman, *Google pays $500 Million to Settle DOJ Case Over Illegal Drug Ads*, CNN MONEY (Aug. 24, 2011), http://money.cnn.com/2011/08/24/technology/google_settlement.

[72] Department of Justice, *supra* note 70.

[73] *Id*.

### *D. Attempts to Regulate Online Speech in the U.S.*

In the United States, case law suggests that the Internet enjoys broad First Amendment rights like those afforded to print media.[74] However, Congress has considered the idea of applying broadcast-like indecency standards to the Internet as part of telecommunications legislation. Congress attempted this through the Communications Decency Act (CDA). The purpose of the broader act was to reduce regulation and encourage "the rapid deployment of new telecommunications technologies."[75] However, the United States Supreme Court held that the anti-indecency provisions of the CDA violated the First Amendment because the regulations were a blanket, content-based restriction on the freedom of speech.[76] The challenged provisions of the CDA sought to protect minors from harmful material on the Internet. The CDA did not limit itself to particular times or individuals. Nor did it recognize the unique nature of Internet communications. Further the CDA did not define "indecent" communications.[77] Courts interpreting the First Amendment distinguish between "indecent" and "obscene" sexual expressions, protecting only those that are indecent.[78]

Advocates of free speech and freedom of information have lobbied legislatures for federal and state net neutrality legislation that would prohibit ISPs from discriminating against any legal content they transmit.[79] In 2007, members of Congress introduced the Internet Freedom Preservation Act of 2007, which would have amended the Communications Act of 1934, making it unlawful for any ISP to "block, interfere with, discriminate against, impair, or degrade the ability of any person to use a broadband service to access, use, send, post, receive, or offer any lawful content, application, or service made available via the internet" or to change on the basis of the type of content the applications or services made

---

[74] KENNETH CREECH, ELECTRONIC MEDIA LAW AND REGULATION 373 (2003).
[75] Reno v. Am. Civil Liberties Union, 521 U.S. 844, 857 (1997).
[76] *Id.* at 868.
[77] *Id.* at 865.
[78] Sable Communications v. FCC, 492 U.S. 115, 126 (1989).
[79] NUNZIATO, *supra* note 61, at 131.

available.[80] Acts by the same name were proposed in 2008 and 2009, yet all have died in Congress. The proposed Blogger Protection Act of 2008 also failed to make it out of committee.[81] This bill would have amended the Federal Election Campaign Act of 1971 to protect uncompensated Internet activity from being treated as a contribution.[82]

The push for net neutrality continues in the United States, despite opposition by interested parties. However, Internet expression has flourished within the U.S. because of laws that provided the Internet industry great protections.[83] Without a law like Section 230 of the CDA, service providers would, at the very least, confront a multitude of lawsuits.[84]

## IV. ESTABLISHING A LEGAL FRAMEWORK FOR PROTECTING INTERNET AS A HUMAN RIGHT

### *A. Essential Elements for a Legal Framework*

Information on the Internet is not confined to the same geographical boundaries as states. Thus, if a state passes laws to control material in its own jurisdiction, this does not stop its citizens from accessing or distributing illegal material through other countries.[85] To be truly effective in blocking all prohibited material, jurisdiction and enforcement would have to be situated at the international level. Governments have come to understand that independent censorship is not as effective as international cooperation.[86] At the international level, the Internet is governed by voluntary codes of practice, public awareness campaigns, education, and other morally persuasive solutions.[87]

---

[80] S. 215, 110th Cong. (2007).

[81] *H.R. 5699 (110th): Blogger Protection Act of 2008*, GOVTRACK.US, http://www.govtrack.us/congress/bills/110/hr5699 (last visited April 8, 2012).

[82] *Id.*

[83] Daithí Mac Síthigh, *The Right to Communicate*, PUBLIUS PROJECT (Nov. 29, 2008), *available at* http://publius.cc/right_communicate.

[84] *Id.*

[85] HUMAN RIGHTS AND THE INTERNET, *supra* note 4, at 160.

[86] *Id.*

[87] *Id.*

A legal framework is not only important out of respect for the rule of law, but it would have a practical impact on the lives of people and on the development of economies. The Internet allows individuals who once had no forum for expression or ability to compete with wealthy, dominant powers to communicate, advertise, and be heard with relatively little cost and fewer barriers than other modes of communication.

We suggest that an international legal framework be adopted to protect the rights of individuals, specifically their freedom of speech and access to the Internet. After review of the existing models, the following factors emerge as essential elements of a legal structure that is successful in protecting freedoms and fostering development. We suggest six factors that all legal systems should incorporate to protect and promote access to the Internet as a human right.

1. Proportionate Response

Any response to online expression should target the objectionable content and not block more information than is necessary, nor should access be denied entirely without just cause. The response should be precisely targeted at the particular matter of concern. Blocking access to the Internet in general should almost never be a response. A government's decision to restrict access to the Internet or content should only target legitimately threatening content that could incite violence or cause a threat to public safety. Also, legal systems should clearly define what activity would be regulated under criminal statutes and what activity should be enforced under a civil system. Criminal punishments for undesirable online content should be limited only to child pornography, hate speech, direct and public incitement to commit genocide, and advocacy of national, racial or religious hatred that incites discrimination or violence.[88] Governments should work to decriminalize defamation and move to a civil legal mechanism.

[88] *See Report of the Special Reporter*, *supra* note 1, at 8-9.

2. Constitutional Protections or Detailed Legislative Regulations

Criteria for which material a government may block and acceptable responses to offending information should be contained in published law. The regulations should be accessible to the public. As was observed above, many of the crackdowns on the Internet under Egypt's prior regime occurred outside the scope of defined law. This cannot be tolerated in a system where rule of law governs and people are able to dispute and challenge the regulations if enforced against them. Freedom of speech and expression online should be adopted as Constitutional protections. States should consider adopting specific laws to ensure that freedom of expression is protected online. States should also adopt programs to help improve access to the Internet, so that it does not become a tool controlled by a powerful few.

3. Neutral Body, Non-corporate Enforcement

A neutral enforcement body should be established to ensure that enforcement does not burden corporations or unequally empower them. The U.N. Special Rapporteur suggests that, to safeguard against abuse, such a body must have no commercial or political affiliations.[89] This body would also serve to protect the growth of Internet companies, because the companies would not be responsible for policing online activity as they would be in a system where they themselves were charged with enforcement.

As the Internet increasingly moves into position as the world's dominant mode of communication, it is a vehicle to spread truth, encourage transparency, hold governments accountable, and uncover corruption. Such a powerful tool should be open, free and accessible. Legal systems should be established to protect it and prevent it from being abused. An independent body charged with the ability to hear evidence and apply clear, nationally established regulations would be best equipped to uphold these ideals. The independent body could operate like an administrative court to weigh evidence for and against writers and posters of online content. This "Internet Court" could then issue decisions about whether online content should be blocked,

[89] *Id.* at 19.

removed, or edited.

4. Judicial Review

The decisions of the "Internet Court" should be appealable to a higher court within the state's existing legal system. A user whose rights have been infringed should have the ability to seek redress in a court of law.

5. Transparency

The criteria for deciding when to enforce restrictions on access and content should be established ex ante and publicized. The process undertaken to decide enforcement actions should also be documented and accessible to the public upon request. The proceedings of any "Internet Court" should be transparent and open to the public. The media should have access to this information in order to inform the public and hold the body accountable.

6. International Approach

In order for any legal system to enforce its regulations on such an international phenomenon as the Internet, it must be cognizant of its place in a broader context. It is just one player in a global web of authorities. Cooperation and partnership between jurisdictions may be the best way to address issues posed by online content. This element of international cooperation also arises because of the space for international conflict over treatment of the Internet.

International Cooperation may take the shape of joint education products or campaigns. It may also involve sharing of evidence and resources between enforcement bodies. As cyberlaw scholar Lawrence Lessig suggests, in order to protect fundamental values, social and legal power is structured and constrained not only by a legal text or constitution but also by a way of life—which he calls an "architecture."[90] He explains:

---

[90] LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 4 (2006).

> To regulate well, you need to know (1) who someone is, (2) where they are, and (3) what they're doing. But because of the way the Internet was originally designed . . . there was no simple way to know (1) who someone is, (2) where they are, and (3) what they're doing. Thus, as life moved onto (this version of) the Internet, the regulability of that life decreased. The architecture of the space—at least as it was—rendered life in this space less regulable.[91]

International enforcement is challenged with creating an Internet culture that is local and personalized, where societal norms apply.

## CONCLUSION

Legal systems should incorporate these six factors in order to elevate as a protected human right a person's freedom to the Internet. This is particularly important as the medium becomes the dominant mode of communication, exchange of thought, and commerce. Internet as a human right serves as a tool, an instrument with which people can work and fight to achieve their other economic, social, cultural, civil, and political rights. It deserves the respect accorded to other human rights and other media.

---

[91] *Id.* at 23.