From the Fringes of Copyright Law: Examining California's "True Name and Address" Internet Piracy Statute

by BRIAN MCFARLIN*

I. Introduction

As high-speed Internet connections have gained popularity, the illegal trading of copyrighted files has quickly become a major issue. Some studies estimate that almost twenty billion songs were illegally downloaded in 2005.[1] Although popular media services, such as Apple's iTunes store, now offer legal copies of songs and videos for download, many Internet users are still stealing copyrighted material.[2] The Recording Industry Association of America (RIAA), an organization representing a conglomerate of music labels in the United States, has been working to

---

* J.D. Candidate 2008, University of California, Hastings College of the Law; B.A. 2004, Political Science and History, University of Michigan. His legal experience has ranged from government work to large and small firms. Beyond the law, his interests include writing, amateur filmmaking, guitar, and discussing fine scotch. He dedicates this note to his parents, who nurtured him with legal knowledge from a young age. He would also like to thank Professor Calvin Massey and the *CLQ* team for their help in editing this note.

1. INT'L FED'N OF THE PHONOGRAPHIC INDUS., THE RECORDING INDUSTRY 2006 PIRACY REPORT 4 (2006), http://www.ifpi.org/content/library/piracy-report2006.pdf. A study also showed that major U.S. motion picture studios lost $6.1 billion in 2005 to piracy worldwide. L.E.K. CONSULTING, THE COST OF MOVIE PIRACY 4 (2006), http://www.fact-uk.org.uk/site/media_centre/documents/2006_05_03leksumm.pdf.

2. At MacWorld in Jan. 2008, Apple announced that it has sold four billion songs, 125 million TV shows, and 7 million movies since the launch of its iTunes store. Bryan Collins, *Apple Launches 'World's Thinnest Notebook,'* ELECTRIC NEWS, Jan. 16, 2008, http://www.electricnews.net/article/10123732.html. However, many services which offer infringing files, such as The Pirate Bay, are as well-known and perhaps even more popular than iTunes and other legitimate services. *See, e.g.*, Dan Mitchell, *Pirates Take Sweden*, N.Y. TIMES, Aug. 19, 2006, at C5.

curb this music piracy by taking legal action against copyright infringers.[3] While the RIAA and their member labels are conflicted on whether lawsuits are the best method for combating Internet piracy, the filing of such suits has continued.[4]

While the RIAA and other such organizations have won many of these suits, one of the major problems they have had with prosecuting pirates of copyrighted material is identifying who is sharing what. Most Internet pirating now occurs on peer-to-peer (P2P) file sharing networks, which are computer networks that enable millions of users to connect with each other and share files.[5] However, recent cases have made it difficult for copyright holders to close down these P2P networks directly.[6] The RIAA and other copyright owners have turned to methods such as using automated web crawlers to scour file sharing networks for the unique Internet Protocol (IP) addresses of those users sharing or downloading copyrighted materials.[7] However, the IP address, by itself, does not have much use because it does not give the name or specific location of the user.[8] Turning this IP address into a name can be nearly impossible.[9] Only the user's Internet Service

3. *See* Hilary Rosen, *For the Record, for What It's Worth*, THE HUFFINGTON POST, June 4, 2006, *available at* http://web.archive.org/web/20070218180330/ http://www.huffingtonpost.com/hilary-rosen/for-the-record-for-what-_b_22177.html.

4. A study suggests that the lawsuits have affected large file-swappers but have had little effect on those who only offer less than 1,000 files and little effect on the availability of files at any given time. *See* Symposium, *Impact of Legal Threats on Online Music Sharing Activity: An Analysis of Music Industry Legal Actions*, 49 J. L. & ECON. 91 (2006). However, a recent stream of legal and legislative successes might suggest that curbing piracy using lawsuits will be more successful in the future. *See* Declan McCullagh, *RIAA's Next Moves in Washington*, CNET NEWS, May 26, 2006, http://news.zdnet.co.uk/ itmanagement/0,1000000308,39271312, 00.htm?r=1.

5. *See* Douglas Heingartner, *Software Piracy Is in Resurgence, with New Safeguards Eroded by File Sharing*, N.Y. TIMES, Jan. 19, 2004, at C9. These P2P networks enable the quick exponential proliferation of files from user to user. For example, once a single user posts a popular copyrighted work, such as a new or as-yet-unreleased movie, P2P technology allows others to download the file from the user and in turn also make it available on the network. With some P2P networks, like BitTorrent, the speed of file transfer actually increases when more users are downloading a file. *See* Carmen Carmack, *How BitTorrent Works*, HOWSTUFFWORKS http://computer.howstuffworks.com/ bittorrent.htm (last visited Mar. 2, 2007).

6. *See, e.g.*, MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (holding that a P2P network defendant who provides infringing material must actually induce the commission of copyright infringements to be convicted).

7. *See* Sonia K. Katyal, *Privacy vs. Piracy*, 9 INT'L J. COMM. L. & POL'Y 7 (2004). The RIAA also has a team of specialists who hunt down pirated content on the Internet and P2P programs. *See* RIAA.com, Piracy: Online and On The Street, http://www.riaa.com/physicalpiracy.php (last visited Feb. 3, 2008).

8. *See* Mikel R. Boeve, *Will Internet Service Providers Be Forced to Turn in Their Copyright Infringing Customers? The Power of the Digital Millennium Copyright Act's Subpoena Provision After* In Re Charter Communications, 29 HAMLINE L. REV. 115, 118-19 (2006).

9. *Id.*

Provider (ISP) can link the IP address to a name, and ISPs, because they wish to protect their customers, are often unwilling to turn this information over without legal action.[10] Also, if an ISP is outside the United States, making use of a court's subpoena power would be difficult, if not impossible.[11]

In response to this problem, Congress passed the Digital Millennium Copyright Act (DMCA) in 1998 to deal with copyright infringement on the Internet and to identify alleged infringers.[12] The DMCA provided a way for copyright holders to issue subpoenas against ISPs to release personal information about alleged copyright infringers.[13] This DMCA subpoena power, unlike more traditional methods of subpoenaing, does not require the approval of a judge in obtaining a warrant.[14]

However, as technology has changed, the DMCA's subpoena power has become mostly worthless, as demonstrated in *RIAA v. Verizon Internet Services*.[15] In *Verizon*, the United States Court of Appeals for the District of Columbia Circuit found that the RIAA could only use DMCA subpoenas against ISPs who are actually storing infringing material on their servers.[16] Since most of today's P2P file sharing software allow users to search and transfer files without the use of a centralized server, the power of copyright holders to subpoena under the DMCA became vastly limited.[17] Copyright holders could still obtain the identity of alleged copyright infringers through other methods, such as a John Doe proceeding, but such a subpoena would require judicial approval and the burden on the copyright holder to justify breaching the anonymity of a defendant would be much

10. *Id.*

11. Converting an IP address into personal information might even require going through several ISPs, which could in turn require several subpoenas and sifting through reams of data. *See* Joel Snyder, *Tracking Internet Piracy: Harder Than You Think*, CIRCLEID, Dec. 31, 2004, http://www.circleid.com/posts/tracking_internet_piracy_harder_than_you_think/. Even if the personal information is found, this only identifies the person who registered with the ISP, not necessarily the copyright infringer. For example, there have been several cases where users charged with Internet piracy have successfully defended against the charge by claiming the piracy was committed by someone else who accessed the users' unencrypted wireless network. *See* Eliot Van Buskirk, *RIAA Fights Back, Threatens Open Wi-Fi*, WIRED BLOG NETWORK (LISTENING POST), Feb. 22, 2007, http://blog.wired.com/music/2007/02/riaa_contests_d.html.

12. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.); *see also* S. REP. NO. 105-90, at 2 (1998).

13. 17 U.S.C. § 512(h) (2006).

14. *Id.*

15. RIAA v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1236-37 (D.C. Cir. 2003).

16. *Id.*

17. *See* David Gorski, *The Future of the Digital Millennium Copyright Act (DMCA) Subpoena Power on the Internet in Light of the Verizon Cases*, 24 REV. LITIG. 149, 165 (2005).

higher than for a DMCA subpoena.[18] Rulings like that in *Verizon*, when combined with the already high cost and large amount of time required to build a case against an alleged copyright infringer, severely limit a copyright holder's options.

Bruised but not beaten, the RIAA and other copyright holders tried to find other ways to easily identify copyright infringers without the limitations presented under the DMCA. One such method involved going outside of federal copyright law entirely and creating new state crimes that mirrored their federal counterparts. In Part II of this article, I will examine one such state law, California Penal Code section 653aa. In Part III, I will explore the constitutional and public policy concerns raised by the statute. In Part IV, I will propose legislation that accomplishes the copyright holder's goal of identifying copyright infringers, but implicates fewer preemption issues and includes better safeguards aimed at protecting individual privacy rights and public safety than does section 653aa.

II. An Overview of California Penal Code Section 653aa

In 2004, California Governor Arnold Schwarzenegger signed into law California Penal Code section 653aa, which became effective on January 1, 2005.[19] Under the statute, anyone located in California who, "knowing that a particular recording or audiovisual work is commercial, knowingly electronically disseminates all or substantially all of that commercial recording or audiovisual work to more than 10 other people without disclosing his or her email address, and the title of the recording or audiovisual work" is guilty of a misdemeanor.[20] The statute defines a "commercial recording or audiovisual work" as "a recording or audiovisual work whose copyright owner, or assignee, authorized agent, or licensee, has made or intends to make available for sale, rental, or for performance or exhibition to the public under license."[21] "Audiovisual work[s]" include motion pictures, television programs, and video or computer games.[22]

The statute provides specific consequences for both minors and adults. Adults are subject to a fine not exceeding $2,500 and/or imprisonment in a

18. A John Doe proceeding is an action where the identity of the defendant is unknown, and the name "John Doe" is assigned to the defendant. Courts, however, have many requirements for allowing such a proceeding. *See* Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 767-68 (N.J. Super. Ct. App. Div. 2001).

19. Mark Martin & Lynda Gledhill, *Governor Signs Internet Privacy Bill, Email Address Required to Share Music, Movies Online*, S.F. CHRON., Sept. 22, 2004, at B2.

20. CAL. PENAL CODE § 653aa(a) (West 2006).

21. *Id.* § 653aa(g)(3).

22. *Id.* § 653aa(g)(2).

county jail for a period not exceeding one year.[23] Minors are only subject to a $250 fine, but, upon a third or subsequent violation, they are punishable by a fine not exceeding $1,000 and/or imprisonment in a county jail for a period not to exceed one year.[24] For both adults and minors the court will order the permanent deletion of the offending file.[25]

There are some exceptions to this rule. Those who only transfer the commercial recording to his or her immediate family or within his or her personal network do not violate the Act.[26] Regardless, such private transfers of infringing material are likely not to apply under the Act because the user would probably not be sharing with ten or more people. Those who have permission or are acting under the authority of the copyright owner are also exempt under the Act.[27] ISPs that enable their users to share files are also exempt if they keep their email address or other means of electronic notification on their website.[28] It is noteworthy, though, that there is no specific exception for fair use of the copyrighted material as there is under federal copyright law.[29]

A stated purpose of the statute was to "allow state law enforcement authorities to pursue copyright violations, since the vast majority of individuals who are using P2P networks to violate copyright law are unlikely to comply with the bill's true name and address requirement."[30] In short, legislators were attempting to build a trap for the unwary designed to allow the state to essentially enforce copyright law in state courts.

Going beyond mirroring federal law, this law actually allows copyright holders to identify pirating users in a way not allowed by federal copyright law. Through this statute, copyright holders have a relatively easy and effective cause of action regardless of whether a copyright infringer chooses to reveal his or her personal information online. If an alleged infringer does embed their physical or email address with the title of the full commercial work to their file, copyright holders can easily find out whether the file is a copyrighted and, if so, directly contact and sue the

23. *Id.* § 653aa(a).

24. *Id.* § 653aa(b).

25. *Id.* § 653aa(e).

26. *Id.* § 653aa(c)(1).

27. *Id.* § 653aa(c)(2).

28. *Id.* § 653aa(f).

29. The fair use doctrine allows, under certain circumstances, the use of copyrighted materials for purposes such as criticism, comment, news reporting, and teaching. *See* 17 U.S.C. § 107 (2006).

30. Senate Judiciary Comm., Bill Analysis of S. 1506, 2003-2004 Leg., Reg. Sess., at 2 (Cal. 2004), *available at* http://leginfo.ca.gov (search 2003-2004 session for Bill Number 1506).

infringer under federal copyright law without having to subpoena their ISP. If an alleged copyright infringer does not include all of this information, she can be held liable under both state criminal law and federal copyright law, provided that the copyright holder is able to identify the infringer.

In addition to allowing easier identification of alleged copyright infringers, section 653aa's state criminal cause of action has other advantages for copyright holders. The statute bypasses many of the limitations of federal copyright law, such as exceptions for fair use.[31] Also, the state cause of action brings in state criminal enforcement resources to aid federal agents in locating copyright infringers.[32] Lastly, the state cause of action allows state courts to adjudicate what are essentially federal copyright issues.

III. Constitutional and Public Policy Issues Arising From California Penal Code Section 653aa

The creation of all of these powers in section 653aa raises serious concerns about the legality of the statute and whether its enforcement would be best for the community and the rights of individuals. Is it really in California's interest to enforce a law that makes it a crime to fail to make your personal information available online? Does the law unduly infringe on the general policies of the state or federal government? Does the creation of a state law touching copyright issues unduly invade upon federal copyright laws? To answer these questions, we must weigh the copyright holder's legitimate interest in maintaining control over their own property against the rights of the individual to maintain their privacy and the rights of the community in deciding on where to allocate the government's limited resources.

A. Constitutional Issues

1. Preemption of California Penal Code Section 653aa by Federal Copyright Law Under Both the Specific Provisions of the Copyright Act of 1976 and General Preemption Doctrines

The United States Constitution, in its Copyright Clause, gives Congress the power to enact statutes "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the

31. *See* 17 U.S.C. § 107 (2006). The fair use exception will be discussed in further detail later in this article. *See infra* Part III.A.1.b.

32. CAL. PENAL CODE § 653aa (West 2006).

exclusive Right to their respective Writings and Discoveries."[33] James Madison affirmed this assertion, stating that, in the area of copyright, "[t]he States cannot separately make effectual provisions . . . ."[34]

While Congress originally allowed states to legislate in this area, they revoked this right through the Copyright Act of 1976, which, with some exceptions, preempted state powers over copyright.[35] The Act was passed pursuant to the Supremacy Clause, which allows the federal government to claim exclusive power to use their enumerated powers.[36] Under the Act, state law cannot provide protection for a work that federal law does not protect.[37]

a. Federal Preemption Under § 301 of the Copyright Act of 1976

Through § 301 of the Copyright Act of 1976, Congress specifically preempted various state copyright laws.[38] Thus, in order to determine whether a specific state law is preempted by federal copyright law, courts usually do not have to resort to standard preemption tests and instead just analyze the statute through the two-pronged test set forth in § 301.[39] First, to be preempted, the state law must create "legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by Section 106."[40] The fact that a state law might offer additional remedies to the federal law does not preclude it from preemption if the right itself is based in federal copyright law.[41] Second, the nature of the works protected in the state law must "come within the subject matter of copyright as specified by Sections 102 and 103 . . . ."[42]

Under the first prong of this test, a state law is subject to preemption if it involves any rights "that are the equivalent of copyright."[43] A right is equivalent to copyright when it is infringed by the mere act of

33. U.S. CONST. art. I, § 8, cl. 8.

34. THE FEDERALIST NO. 43 (James Madison).

35. Copyright Act of 1976, Pub. L. No. 94-553, § 301, 90 Stat. 2541, 2572 (codified as amended at 17 U.S.C. § 301 (2006)). Some of these exceptions include common law copyright violations and, as I will discuss later, state laws respecting sound recordings fixed before Feb. 15, 1972. *Id.*

36. U.S. CONST. art. VI, § 2.

37. *See* H.R. REP. NO. 94-1476, at 131 (1976).

38. 17 U.S.C. § 301 (2006).

39. *See* Hillsborough County v. Automated Med. Labs, Inc., 471 U.S. 707 (1985).

40. 17 U.S.C. § 301 (2006).

41. *See* Pena-Rivera v. Editorial Am., S.A., 43 U.S.P.Q.2d (BNA) 1059, 1061 (S.D. Fla. 1997).

42. *Id.*

43. H.R. REP. NO. 94–1476, at 130 (1976).

reproduction, performance, distribution, or display.[44] However, if other material elements are required in addition to these acts in order to create a cause of action under the state law, then there is no preemption under the Copyright Act.[45] To avoid preemption, the additional elements in the state law "must regulate conduct qualitatively different from the conduct governed by federal copyright law."[46] This means that if a state law merely duplicates the typical copyright violations already covered by federal law, the state law is preempted and is invalid.

Whether California's "True Name and Address" statute is preempted under the first prong of § 301 hinges on whether its additional elements are considered material. Section 653aa, like federal copyright law, protects the right of copyright holders to prevent the unauthorized distribution of their works. Unlike federal law, though, this statute adds a requirement that the copyrighted work must be distributed with the infringer's name and address. The statute also adds the requirements that the conduct is "knowing" and that the works distributed are "commercial." While section 653aa's penalty is allegedly for refusing to provide the proper information, a closer look reveals that these additional elements might not be sufficient enough to avoid preemption under § 301's first prong.[47] The true legislative intent behind section 653aa was to prevent the unauthorized copying, distributing, or displaying of a copyrighted work.[48] This means

44. Trandes Corp. v. Guy F. Atkinson Co., 996 F.2d 655, 659 (4th Cir. 1993).

45. *Id.* Under this test, for example, contract and trade secret law claims are typically not preempted even if the breach involves copyright because they require proof of an additional element (e.g., an agreement or a confidential relationship). *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996); Computer Assoc. Int'l, Inc. v. Altai, Inc., 982 F.2d 693 (2d Cir. 1992).

46. *Trandes Corp.*, 996 F.2d at 659.

47. Whether these additional elements are sufficient for section 653aa to escape federal preemption is a close call. "This effort [in section 653aa] to address issues created by so-called peer-to-peer online technology reflects reasonable policy considerations, but very likely encounters preemption issues. The subject matter involved is clearly copyrightable subject matter. The wrongful acts involve copying and distribution—exclusive rights under copyright law. The preemption issues will lie in whether the requirements of 'knowing' conduct, 'commercial' works, and failing to provide an email address and title are a sufficiently quantitative extra element to take the statute out of the range of preemption. The issue is very close." RAYMOND T. NIMMER & HOLLY TOWLE, THE LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS § 3.07 (2003 & Supp. 2005). At least one court suggests that "the additional elements of 'knowledge' and 'intent' required under state law do not afford plaintiff rights that are 'different in kind' from those protected by the copyright laws." Harper & Row, Publishers, Inc. v. Nation Enters., 501 F. Supp. 848, 854 (S.D.N.Y. 1980).

48. "[Senator] Murray says the point isn't to take names; his idea is to give state prosecutors, who have no jurisdiction over copyright infringement, a charge they can bring against online pirates." Jim Healy, *Setting a Trap for Net Pirates*, L.A. TIMES, Mar. 17, 2004, at C1.

that the state law is essentially punishing conduct that is already regulated under federal copyright law. Furthermore, the entire purpose of the act is to make it easier for the RIAA and other copyright holders to identify and sue copyright infringers under federal law.[49] Someone being charged under section 653aa is essentially being prosecuted for copyright infringement under state law as a means for bypassing federal copyright laws, a result which conflicts with Congress's intent to have exclusive federal power over copyright law. The conduct being regulated by section 653aa does not seem to be qualitatively different than the conduct regulated under federal copyright law, so it might be considered the "equivalent of copyright."

It is true that forty-five states, including California, already have long-standing, presumably legitimate statutes that are, in some respects, similar to section 653aa.[50] These statues typically require that the true name and address of the manufacturer be printed on sound recordings intended for sale or rental.[51] In *Anderson v. Nidorf*, the Ninth Circuit affirmed a conviction under California Penal Code section 653w, which required disclosure of the true name and address of the manufacturer of any audiotape or videotape offered or possessed for the purposes of sale, in spite of claims that it was preempted by federal copyright law.[52] The court reasoned that since the statute "does not prohibit the reproduction of copyrighted works, but rather prohibits selling recordings without disclosing the manufacturer and author of the recording (regardless of its copyright status), the federal copyright laws do not preempt the state statute."[53] The court also found that since the statute was not just designed to protect copyright owners, but was also meant to protect consumers from deceptive commercial practices, it incorporated material elements beyond federal copyright law, as required under § 301 of the Copyright Act of 1976.[54]

However, the reasoning used by the Ninth Circuit in *Nidorf* to reject the federal preemption argument is not as persuasive when applied to section 653aa. One could analogize to *Nidorf* and claim that section 653aa does not prohibit the reproduction of copyrighted works, but merely prohibits Internet file sharers from distributing commercial works without

49. *See* Senate Judiciary Comm., Bill Analysis of S. 1506, 2003-2004 Leg., Reg. Sess., at 2 (Cal. 2004), *available at* http://leginfo.ca.gov (search 2003-2004 session for Bill Number 1506).

50. MPAA.org, Piracy and the Law - State Law, http://www.mpaa.org/piracy_ StateLaw.asp (last visited Feb. 21, 2007).

51. *Id.*

52. Anderson v. Nidorf, 26 F.3d 100, 102 (9th Cir. 1993).

53. *Id.*

54. *Id.*

disclosing the sharer's true name and address. Unlike in the section 653w statute examined in *Nidorf*, though, section 653aa only targets copyrighted files and does not involve any commercial transactions.[55] Without these two key additional material elements that protect interests outside of federal copyright law, section 653aa does not fare as well as section 653w on the first prong of a § 301 analysis. Also, unlike section 653w, which the Ninth Circuit claimed was also meant to accomplish the state interest in protecting consumers from unknowingly receiving bootleg merchandise, section 653aa is only intended to protect the interests of copyright holders, a distinctly federal interest.[56] The legislative history confirms this assertion as it does not show any legislative intention beyond protecting copyright interests.[57] The Internet piracy that section 653aa regulates does not involve any illicit financial gain from sellers or consumer fraud; the only party that really needs protection from such a transaction is the copyright holder.

Since section 653aa does not involve the material elements apparent in statutes like section 653w, and the essential purpose of section 653aa is to protect copyright, it is probable that a court would find that section 653aa violates the first prong of the § 301 test.

Under the second prong of the § 301 test, the works covered under section 653aa must fit within one of the general subjects enumerated in § 102 or § 103 of the Copyright Act.[58] Section 102 of the Copyright Act specifically mentions "motion pictures and other audiovisual works," which includes movies, television programs, and video games.[59] This would coincide with section 653aa's coverage of "audiovisual works." "Sound recordings" are also listed in § 102 of the Copyright Act, which

55. CAL. PENAL CODE § 653aa (West 2006).

56. *Nidorf*, 26 F.3d at 102.

57. *See* Senate Judiciary Comm., Bill Analysis of S. 1506, 2003-2004 Leg., Reg. Sess., at 2 (Cal. 2004), *available at* http://leginfo.ca.gov (search 2003-2004 session for Bill Number 1506). The Motion Picture Association of America (MPAA) claimed in support of the section 653aa that the bill would also "alert California consumers from whom they are downloading files, in case the files contain viruses or other harms, or may be counterfeit." *Id.* at 4. However, the bill does not accomplish this objective because it is unlikely that a user sharing a file with virus or a counterfeit file will choose to share their personal information. Also, it is unclear what action, if any, a user could or would want to take once they downloaded a copyrighted file with a virus if they have the file sharer's personal information. Regardless, the legislative history does not show that the legislature considered this to be a purpose of the statute.

58. *See* Crow v. Wainwright, 720 F.2d 1224 (11th Cir. 1983) (holding that application of a criminal law prohibiting dealing in stolen property to sale of pirated sound recordings was preempted by the Copyright Act).

59. 17 U.S.C. § 102 (2006).

would coincide with the "music files" mentioned in section 653aa.[60] However, as § 301(c) of the Copyright Act notes, "[w]ith respect to sound recordings fixed before February 15, 1972, any rights or remedies under the common law or statutes of any State shall not be annulled or limited by this title until February 15, 2067."[61] This means that "state prosecutions for criminal activity with respect to copyright infringement are, of course, preempted, except as regards pre-1972 sound recordings."[62] Thus, California Penal Code section 653aa is invalid under this prong, at least when applied to sound recordings fixed after the 1972 date. Other penal statues dealing with violations of copyright for sound recordings, such as California Penal Code section 653h, often specify that they do not apply to recordings after the 1972 date, but section 653aa has no such provision and, as such, runs into problems with the second prong of the § 301 test.[63]

Section 653aa, at its heart, imposes criminal penalties for infringing upon copyright without the addition of other material elements and covers copyrighted works over which Congress has claimed exclusive federal jurisdiction. As a result, it seems that section 653aa is preempted by federal law under § 301 of the Copyright Act of 1976 except for its application to sound recordings fixed before February 15, 1972.

b. Federal Preemption Under General Preemption Doctrines

In addition to finding federal preemption under specific statutory provisions like § 301, courts can also analyze state statutes under the regular preemption doctrines.[64] Under these doctrines, a state law that frustrates specific provisions of the federal Copyright Act is preempted.[65]

Since section 653aa has the effect of essentially convicting people of copyright infringement under state law in instances where they would be

60. *Id.*

61. *Id.* § 301(c).

62. WILLIAM F. PATRY, LATMAN'S THE COPYRIGHT LAW 295 (6th ed. 1986).

63. Cal. Penal Code § 653h (West 2006). Section 653(h) is typical of state statutes dealing with sound recordings. "[F]ederal preemption does not apply to sound recordings fixed earlier than February 15, 1972; therefore, most states have enacted statutes to protect copyright interests in pre-1972 recordings." Timothy D. Howell, *Intellectual Property Pirates: Congress Raises the Stakes in the Modern Battle to Protect Copyrights and Safeguard the United States Economy*, 27 ST. MARY'S L.J. 613, 667 n.199 (1996).

64. *See* Geier v. Am. Honda Motor Co., 529 U.S. 861, 869-74 (2000) (holding that the express preemption clause in the Motor Vehicle Safety Act of 1966 does not bar the ordinary working of conflict preemption principles).

65. *See, e.g.*, Avtec Sys., Inc. v. Peiffer, 21 F.3d 568, 574-75 (4th Cir. 1994) (holding that a copyright owner cannot be prohibited from exercising his right under federal law to publish his work, simply by virtue of an allegation that the material contained therein constitutes another's trade secret, protected under state law).

innocent under federal copyright law, the act does frustrate certain provisions in federal Copyright Act. For example, section 653aa does not offer the same exceptions for fair use as federal copyright law does. Under federal law, "the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright."[66] The fair use doctrine is an equitable rule of reason which takes into account a set of criteria, including the purpose and character of the use, the nature of the copyrighted work, and portion of the work used, and the effect of the use on the market.[67]

Although section 653aa only applies to the sharing of substantial portions of a copyrighted work, there are no other references to other fair use considerations and there is no mention of fair use as an exception or defense to the statute.[68] Since the statute creates a state criminal cause of action, federal copyright law and its fair use exception do not apply. This means that a user sharing copyrighted work on the Internet for "fair use" would be liable under section 653aa, but not under federal copyright laws. For example, electronically disseminating the incidental reproduction, in a newsreel or broadcast, of work located in the scene of an event being reported would be legitimate "fair use" under federal copyright law, but would violate section 653aa.[69] By effectively excluding the "fair use" protections which Congress saw fit to provide alleged copyright infringers, section 653aa frustrates a specific provision of the federal Copyright Act and thus is preempted by federal law even under general preemption doctrines.

2. Preemption of California Penal Code Section 653aa by Federal Statutes Involving a Minor's Right to Privacy Online and Protection from Unsolicited Commercial Emails

Not only does the California "True Name and Address" statute run into preemption problems with federal copyright law, but it also potentially runs afoul of federal laws designed to protect Internet privacy, especially those dealing with minors and with unsolicited emails. Whether section 653aa is actually preempted by these federal laws must be determined by studying each of the statutes. Preemption may apply whenever federal

66. 17 U.S.C. § 107 (2006).

67. *Id.*

68. CAL. PENAL CODE § 653aa (West 2006).

69. H.R. REP. NO. 94-1476, at 65 (1976).

power is validly exercised to legislate.[70] When analyzing a federal law, courts tend to presume that it is not intended to preempt state law, especially when the power is one traditionally left to the states.[71]

When this intent is manifested, however, it can either be done expressly or impliedly.[72] Express preemption requires specific language in the federal statute that defines the preemption's existence and scope.[73] Implied preemption can be found either when the federal law was intended to occupy an entire field or when it conflicts with the state law, either through impossibility or because the state law is an obstacle.[74] Intent to occupy an entire field can be inferred by creating pervasive federal regulation of that field, by touching a field in which the federal interest is sufficiently dominant to preclude state laws, or through the nature of the purpose of the federal law.[75] Impossibility preemption occurs when complying with both state and federal law is physically impossible.[76] A state law is an obstacle to a federal law when it "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[77] Obstacle preemption is often found when the state law discourages behavior that federal law specifically encourages.[78] However, it will not be found simply because the state law is in "general tension with the broad or abstract goals that may be attributed to various federal laws or programs."[79]

a. The Children's Online Privacy Protection Act of 1998 (COPPA)

In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA), which dealt with concerns over the online collection of

70. CALVIN R. MASSEY, AMERICAN CONSTITUTIONAL LAW: POWERS AND LIBERTIES 316 (2d ed. 2005).

71. Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 96-97 (1992).

72. MASSEY, *supra* note 70, at 316.

73. *Id.*

74. *Id.* at 317.

75. *Id.*

76. *Id.*

77. Hines v. Davidowitz, 312 U.S. 52, 67 (1941). *See also* McDermott v. Wisconsin, 228 U.S. 115, 132 (1913) ("[T]o the extent that the state law interferes with or frustrates the operation of the acts of Congress, its provisions must yield to the superior Federal power given to Congress by the Constitution.").

78. *See* Nash v. Fla. Indus. Comm'n, 389 U.S. 235 (1967) (holding that a Florida law refusing unemployment benefits to any person unemployed as a result of a labor dispute was an obstacle to the federal objective of encouraging compliance with federal labor laws).

79. LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 487 (2d ed. 1988).

personal information from children, especially from commercial websites.[80] COPPA states that "it is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child" unless it provides notice of doing so on their website or it obtains verifiable parental consent.[81] "Children" are defined as those under the age of thirteen.[82] "Personal information" includes a first and last name, a home or physical address, or an email address.[83]

COPPA has an explicit preemption clause which states that "[n]o State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section."[84] However, this clause does not apply here because section 653aa only imposes liability on minors, not the website operators who might obtain their information.

It is possible, though, that COPPA implicitly preempts section 653aa through congressional intent to occupy the field of protecting a minor's right to privacy online. Even though privacy laws are not exclusively federal, the purpose of the interest at stake in COPPA is of a nature that would benefit from federal regulation.[85] Because of the global nature of the Internet, any laws dealing with it are more effective if they cover a large jurisdiction. In the case of COPPA, having piecemeal and contradictory laws from state to state on the issue would make it difficult for violators of a minor's right to privacy to be prosecuted. Most instances in which a minor's right to privacy is violated over the Internet are going to involve parties from different states, so allowing separate state laws in the field would defeat the purpose of COPPA. Since section 653aa cannot operate without impairing Congress and COPPA's ability to operate in its field, this might suggest that section 653aa is preempted.[86]

---

80. Children's Online Privacy Protection Act, 15 U.S.C. § 6502 (2006).

81. *Id.*

82. *Id.* § 6501.

83. *Id.*

84. *Id.* § 6502.

85. *See, e.g.*, CAL. BUS. & PROF. CODE § 22575 (West 2006).

86. *See* Fla. Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142 (1963) ("The test of whether both federal and state regulations may operate, or the state regulation must give way, is whether both regulations can be enforced without impairing the federal superintendence of the field, not whether they are aimed at similar or different objectives."). *See also* San Diego Bldg. Trades Council v. Garmon, 359 U.S. 236, 244 (1959) ("Regardless of the mode adopted, to allow the States to control conduct which is the subject of national regulation would create potential frustration of national purposes.").

However, since courts tend to construe narrowly the field which a federal law occupies in order to prevent a legislative vacuum, these arguments might not be enough to convince a court to find that section 653aa is subject to field preemption.[87] More specifically, COPPA only restricts the ways in which commercial site owners can knowingly gather information from minors.[88] Section 653aa, on the other hand, forces minors to divulge their information on file sharing networks, which are not commercial sites and do not collect personal information.[89] Also, COPPA already has a specific preemption clause that does not specify a field wide enough to preempt section 653aa, which confirms that Congress likely did not intend a statute like section 653aa to be preempted by COPPA. As a result, it is likely that a court will not find that section 653aa unduly intrudes on the "field" protected under COPPA.

In addition to field preemption, one could argue that section 653aa is a considerable barrier to the purposes of COPPA and therefore fits under obstacle preemption. It defeats the purpose of COPPA to have a state statute that forces minors, under threat of fine and imprisonment, to provide their personal information online, regardless of parental consent, in a way that is accessible to all Internet users, including the site operators that COPPA is attempting to restrict. Basically, section 653aa uses state law to defeat the very interests that COPPA is trying to protect. However, this does not necessarily mean that section 653aa is preempted under this analysis. As mentioned earlier, COPPA liability is aimed at website operators, while section 653aa liability is aimed at minors. As a result, whether obstacle preemption is found here depends on whether a court would construe the purposes of COPPA wide enough to find that section 653aa is a significant obstacle to that purpose.

There is no impossibility preemption here because it is not physically impossible for a minor to comply with both section 653aa and COPPA. Even if a minor decides to share a copyrighted work online and complies with section 653aa by disclosing his or her personal information, he or she is not specifically violating COPPA. COPPA is violated by owners of commercial websites, not the minors themselves.[90]

In short, the strongest argument for preemption of section 653aa under COPPA would be obstacle preemption, but there is a lot of wiggle room for a court to go either way on this issue. Some considerations would be how

87. MASSEY, *supra* note 70, at 317.

88. 15 U.S.C. § 6502.

89. CAL. PENAL CODE § 653aa (West 2006).

90. 15 U.S.C. § 6502

wide to imply the scope of COPPA's purpose and preemption field and how large a frustration of that purpose is needed to warrant preemption.

b. CAN-SPAM Act of 2003

Section 653aa also has potential preemption issues with federal acts designed to lower the number of unsolicited commercial emails sent to users' accounts. One such statute, the CAN-SPAM Act of 2003, created a unified federal system regulating the sending of spam, or unsolicited commercial email.[91] After looking at studies, Congress found there was "a substantial government interest in regulation of commercial electronic mail on a nationwide basis."[92] In response, the CAN-SPAM Act made it unlawful to send spam emails to email addresses automatically obtained from a website or other online service where the website or service has a posted privacy policy stating that they will not transfer addresses from their site to another party.[93] The Act also banned sending spam emails containing fraudulent header information,[94] required the inclusion of certain information in spam email,[95] and prohibited sending further spam emails to those users who have chosen to opt-out of receiving further communication.[96]

The CAN-SPAM Act, like COPPA, has a specific preemption clause, this one including preemption of any state statute that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[97] The Act also specifies that it should not be construed to preempt "state laws that are not specific to electronic mail."[98] Since section 653aa does not directly regulate the use of electronic mail, it would not fall under the Act's explicit preemption.

The explicit preemption clause also makes it unlikely that Congress intended to "occupy the field" of spam regulation to the point of preempting a state statute like section 653aa, which does not purport to deal with spam email. One could make field preemption arguments similar to

91. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, 15 U.S.C. § 7701 (2006).

92. *Id.* § 7704.

93. *Id.*

94. 18 U.S.C. § 1037.

95. 15 U.S.C. § 7704.

96. *Id.*

97. *Id.* § 7707.

98. *Id.*

those made for COPPA, but since courts tend to narrowly view the field occupied by a federal statute, it is unlikely that a court would find that section 653aa is invalidated through a field preemption analysis.

There is, however, a tenable argument that section 653aa is an obstacle to the objectives of the CAN-SPAM Act. One of the purposes of the Act is to prevent the sending of spam to email addresses automatically obtained from websites and other online services.[99] Since section 653aa requires users of P2P networks, which are online services, to append their full names and email or physical addresses to "commercial works," it can conflict with that purpose. Compliance with section 653aa would vastly increase the number of email addresses available on P2P networks for spammers to automatically gather, effectively promoting the sending of more spam emails. Like with obstacle preemption under COPPA, though, whether there is preemption depends largely on how broadly one defines the purposes of the federal statute. If viewed narrowly, CAN-SPAM targets those who send spam emails, while section 653aa targets copyright infringers. This view seems unduly narrow, though, so it is certainly possible that a court would find that the CAN-SPAM Act preempts section 653aa.

3. Privacy Issues

Section 653aa forces file sharers to put their real names and addresses on all "commercial work" files they trade. This creates questions on whether section 653aa violates privacy rights created under the United States Constitution or the California Constitution.

a. The Right of Privacy in the United States Constitution

The United States Constitution does not specifically mention any right of privacy.[100] However, the United States Supreme Court has found that the right to privacy is an implied fundamental right guaranteed by the Constitution.[101] In *Whalen v. Roe*, the Supreme Court held that the interest of privacy includes "the individual interest in avoiding the disclosure of personal matters."[102] This "informational privacy" is frequently interpreted as a property interest over one's personal information.[103] However, it is unclear whether the *Whalen* Court intended informational privacy to be a

99. *Id.* § 7701.

100. Roe v. Wade, 410 U.S. 113, 152 (1973).

101. *Id.*

102. Whalen v. Roe, 429 U.S. 589, 599 (1977).

103. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000).

mere constitutional interest or an actual constitutional right.[104] While a constitutional interest in informational privacy could be outweighed by the government's need for the information, a constitutional right in informational privacy could only be set aside when outweighed by a compelling government interest or a competing constitutional right.[105]

Many lower federal courts, however, have interpreted informational privacy as a constitutional right.[106] The majority of these courts have weighed privacy and government interests in a general balancing test that uses some form of heightened scrutiny.[107] The Ninth Circuit, for example, balances "the government's interest in having or using the information against the individual's interest in denying access."[108] The Ninth Circuit also stated that "[t]he government may seek and use information covered by the right to privacy if it can show that its use of the information would advance a legitimate state interest and that its actions are narrowly tailored to meet the legitimate interest."[109] Under such tests, though, there have been few cases where the government's interests were outweighed by privacy interests and this often only occurred when the government has compelled disclosure of highly personal or sensitive information.[110] How personal or sensitive the information must be to create a privacy interest is unclear.[111] Some courts have held there is at least some privacy protection for home addresses, but the expectation of privacy for that kind of information is fairly low.[112]

In *Whalen*, the Court examined a New York statute which required physicians to identify patients obtaining Schedule II drugs, a class of drugs having a potential for abuse.[113] This information would be recorded to a centralized computer file maintained by the state Department of Health.[114] The plaintiffs, some of them patients, claimed that the statute violated their

104. *See* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1125 (2002).

105. *Id.*

106. *Id.* at 1126. However, the Fourth and Sixth Circuits have not recognized informational privacy as a constitutional right. *Id.*

107. *Id.*

108. Doe v. Att'y Gen. of U.S., 941 F.2d 780, 796 (9th Cir. 1991).

109. *Id.*

110. Lin, *supra* note 104, at 1127.

111. *Id.*

112. *See, e.g.*, Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999) ("We are not insensitive to the argument that notification implicates plaintiffs' privacy interest by disclosing their home addresses.").

113. Whalen v. Roe, 429 U.S. 589, 593 (1977).

114. *Id.*

federal constitutional right to privacy because misuse of the computer data could cause a leak to the public that would stigmatize them as drug addicts.[115] The Court, however, held that the government interest in disclosure of this medical information to state agencies concerned with public health was essential and was within the state's broad police powers.[116] The Court also found that the possibility of abuse of the statute did not implicate any constitutionally recognized right of privacy.[117] There was no support for the claim that security provisions would be inadequately administered and there had been no such abuse in the past.[118] Since there was no protected privacy interest, the Court found that the state's essential interests outweighed any potential for abuse.[119]

When analyzing section 653aa, we must balance the privacy interests at stake against the state's legitimate objectives. As discussed above, some lower courts have recognized an inherent, if weak, privacy interest in one's address.[120] In the instance of section 653aa though, this interest is heightened by several factors. First, section 653aa forces the inclusion of the person's full name, which, with the address, further identifies the individual. Second, unlike in *Whalen*, where public disclosure would only occur if the statute's safeguards on the information were abused, section 653aa inherently forces public disclosure of personal information. Lastly, there is an intrinsic stigma associated with the disclosure. It is likely that, in an attempt to avoid violating section 653aa, Internet users would attach their personal information to many files that they share on P2P networks, even if they are not "commercial works" under the statute. Even if Internet users follow section 653aa to the letter, they can be forced to disclose their identity in situations where they are not violating federal copyright law, such as when they are complying with the federal "fair use" exception. The disclosure of information in these cases carries with it the unjustified public stigma that the person in question is a copyright infringer, even though they might not have committed any crime.

This privacy interest is counterbalanced by strong state interests. States have a legitimate and broad interest in exercising their police powers.[121] Whether section 653aa's copyright issues are a proper goal for

115. *Id.* at 595.

116. *Id.* at 602.

117. *Id.* at 603-04.

118. *Id.* at 601.

119. *Id.* at 602.

120. *See* Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999).

121. *Whalen*, 429 U.S. at 597 ("State legislation which has some effect on individual liberty or privacy may not be held unconstitutional simply because a court finds it unnecessary, in whole

the states to deal with, as opposed to the federal legislature, is a complex question and is addressed earlier in this Note. Regardless, there is certainly a strong societal interest in the protection of copyright ownership and section 653aa allows the government to better identify those who are violating copyright laws. However, it is questionable whether section 653aa is narrowly tailored to meet that interest. While the statute helps to expose the identities of alleged copyright violators, it also publicly exposes those who have not even violated federal copyright law, as discussed above. Also, the state has no authority to regulate copyright, especially when that regulation is inconsistent with the copyright laws passed by Congress, who has exclusive jurisdiction over the issue.

Whether a full name and address are considered private and sensitive enough under these circumstances to outweigh the state's interests is unclear. The Supreme Court has not confirmed a constitutional right to informational privacy and has not presented a clear test of when such an interest would be violated.[122] However, considering the decisions of the lower federal courts, there at least seems to be enough of a privacy interest involved with section 653aa to make a good argument that it violates the federal constitutional right to privacy.

b. The Right of Privacy in the California State Constitution

The California State Constitution, unlike the United States Constitution, has an explicit right of privacy.[123] In fact, it has the most protective state constitutional provision for privacy.[124] The provision provides all Californians the rights of "enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[125] California's right to privacy, unlike the federal right, clearly includes informational privacy under its wing and provides specific protections to enforce it.[126] In fact, courts have confirmed that California's privacy right "exists to prevent governmental snooping, to inhibit the overly broad collection and retention of unnecessary personal information or the improper use of information

---

or in part. For we have frequently recognized that individual states have broad latitude in experimenting with possible solutions to problems of vital local concern.").

122. Lin, *supra* note 104, at 1125.

123. *See* Am. Acad. of Pediatrics v. Lungren, 16 Cal. 4th 307, 326 (Cal. 1997). This explicit right "protects a larger zone of privacy in the area of financial and personal affairs than the federal right . . . ." Wilson v. Cal. Health Facilities Comm'n, 110 Cal. App. 3d 317 (Cal. Ct. App. 1980).

124. Lin, *supra* note 104, at 1131.

125. CAL. CONST. art. I, § 1.

126. Lin, *supra* note 104, at 1133.

properly obtained for a specific purpose, and to avoid the evils incident to lack of a reasonable check on the accuracy of existing records."[127]

To find an invasion of privacy under the California Constitution, a court must find that the claim satisfies three elements.[128] First, the plaintiff must identify a "specific, legally protected privacy interest."[129] One such general interest is in "precluding the dissemination or misuse of sensitive and confidential information."[130] Information is private "when well-established norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity."[131] These norms are determined from the law governing the right to privacy.[132] Second, there must be a reasonable expectation of privacy under the circumstances, which partially is dependent on the specific circumstances of the case.[133] A reasonable expectation of privacy is found when there is "an objective entitlement founded on broadly based and widely accepted community norms."[134] Lastly, the defendant's conduct must constitute a serious invasion of privacy that is "an egregious breach of the social norms underlying the privacy right."[135] However, even if an incursion into individual privacy is found under the three elements, it can be justified if outweighed by legitimate and important competing interests.[136] The force of the compelling interests is lessened if there are effective alternatives to the violating conduct that would have a lesser impact on privacy.[137] Outside of these three elements, though, the kind of privacy interest involved and the nature of seriousness of the invasion remain the critical factors in the analysis.[138] When a privacy interest is not fundamental, a general balancing of interests is involved.[139]

Under the first element, one must show that section 653aa's forced disclosure of a file sharer's full name and physical and/or email address violates a legally protected privacy interest. In general, California courts

127. Richards v. Super. Ct., 86 Cal. App. 3d 265, 273 (Cal. Ct. App. 1978).
128. Hill v. NCAA, 7 Cal. 4th 1, 35 (Cal. 1994).
129. *Id.*
130. *Id.*
131. *Id.*
132. *Id.* at 36.
133. *Id.*
134. *Id.* at 37.
135. *Id.*
136. *Id.* at 38.
137. *Id.*
138. *Id.* at 34.
139. *Id.*

seem to have recognized a person's address to involve such an interest. In *Fredenburg v. City of Fremont*, the plaintiff challenged the disclosure of the general location of sexual predators on the Internet pursuant to California's Megan's Law.[140] The California Court of Appeal found that there was no federal or state privacy right over the general location of one's residence.[141] The court also found, in dicta, that even if the law forced the disclosure of people's specific addresses, the privacy interests at stake were outweighed by the Act's purpose of informing the public for its own safety.[142] This would suggest that when a law compels disclosure of an individual's specific physical address, there is a legitimate privacy interest and the interest must be balanced against the government's compelling objectives.

In the specific instance of section 653aa, this assertion is bolstered by the fact that, unlike the hypothetical law discussed in the dicta of *Fredenburg*, section 653aa requires disclosure of a name along with the address, which specifically identifies the individual in question and thus increases the privacy interest. Also, as discussed earlier under the federal privacy right analysis, there is, under certain circumstances, an unjustified stigma in the forced disclosure of information under section 653aa where the user has not actually violated federal copyright law. In these instances, the forced disclosure publicly labels the individual as a copyright infringer when they have done no wrong. Such a stigma, when undeserved, certainly involves the "unjustified embarrassment or indignity" required to prove the existence of a legally protected privacy interest.

The second element requires that section 653aa's forced disclosure violates an individual's reasonable expectations of privacy. "[C]ustoms, practices, and physical settings surrounding particular activities may create or inhibit expectations of privacy."[143] The forum in which section 653aa governs is the Internet, which, in terms of privacy, is a unique place. Any information posted publicly on the Internet is instantly available to the entire world. Because of this, many Internet users are highly concerned about posting their personal information online.[144] Even social networking sites, such as MySpace, respect this need for privacy and hide full names

140. Fredenburg v. City of Fremont, 119 Cal. App. 4th 408, 418 (Cal. Ct. App. 2004).

141. *Id.* at 422.

142. *Id.* at 421-22.

143. *Hill*, 7 Cal. 4th at 36.

144. Ninety-two percent of Americans say they are concerned about threats to their personal privacy when they use the Internet and sixty-seven percent say they are "very concerned." FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 2 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

and email addresses from others outside the user's personal network.[145] While many individuals accept publishing their full names and addresses in other public forums, such as a telephone directory, they are more hesitant to do so on the Internet, where there is a heightened interest in being able to present opinions anonymously.[146]

However, some factors might diminish this expectation of privacy. First, "advance notice of an impending action may serve to limit an intrusion upon personal dignity and security."[147] Since section 653aa gives notice that those sharing commercial works will be required to disclose their personal information, there is arguably a lesser expectation of privacy. Next, studies have found that the vast majority of websites collect some type of personal information, so perhaps the disclosure that section 653aa requires is not unusual enough to violate a reasonable expectation of privacy.[148] However, in instances where websites collect personal information, the disclosure of such information is voluntary and the information is often only viewable by the administrators of the website in accordance with the website's privacy policy. In the case of section 653aa, though, the disclosure is completely public and involuntary. Overall, even though the statute provides notice and many websites collect information, it seems fair to say that an individual probably has a reasonable expectation of privacy in not being forced to disclose their full name and address to the public when on the Internet.

For the third element, the privacy interests implicated by section 653aa must be serious enough to constitute an egregious breach of social norms. The terms of this element are unclear, and probably intentionally so. A court could certainly go either way on this issue. On one hand, disclosing a full name and address on the Internet opens an individual up to possible harassment and embarrassment, especially since a disclosure under section 653aa carries with it the stigma that the individual is a copyright violator. On the other hand, the privacy interest is not particularly fundamental. The disclosure, while embarrassing, does not reveal any highly sensitive information. A person's full name and address often can be found in many places, such as a telephone book or a school directory,

145. "With the exception of inviting friends, adding friends, and notifications, a user's email address is not shared or displayed to people within a user's personal network." MySpace.com, Privacy Policy, http://www.myspace.com (follow "Privacy" hyperlink at bottom of page).

146. Seventy-six percent of "consumers who are not generally concerned about the misuse of their personal information fear privacy intrusions on the Internet." FTC, *supra* note 144, at 2.

147. *Hill*, 7 Cal. 4th at 36.

148. Ninety-seven percent of the sites in the study's random sample collected "an email address or some other type of personal identifying information." FTC, *supra* note 144, at 9.

but this disclosure is voluntary, unlike the forced disclosures in section 653aa. Whether the privacy interests intertwined with section 653aa's forced disclosure are "serious" is matter of interpretation. However, if forced to guess, I would think a court would decline to find that the privacy violation here is serious enough.

If a court does find that all three elements have been met, it still can justify the privacy violation if it is outweighed by a legitimate state interest. Here, as mentioned earlier in my analysis of the federal right of privacy, there is a strong social interest in protecting intellectual property. Businesses in the United States depend on copyright law to maintain control over and profit from their intellectual works. One could question, though, whether section 653aa really serves a legitimate interest at all, since it deals with copyright issues specifically reserved for Congress, not the states.

These state interests also can be served by effective alternatives to section 653aa that have less of an impact on privacy interests. Section 653aa was designed originally to circumvent the subpoena process built into federal copyright law, which required a plaintiff to fulfill certain requirements to obtain the personal information of a suspected copyright infringer.[149] The subpoena process is designed to ensure that a plaintiff has sufficient evidence before forcing the disclosure of an individual's private information.[150] If copyright owners such as the RIAA wish to be able to obtain information more easily on copyright infringers, it should be through such a subpoena, not a law like section 653aa. Since effective alternatives exist that involve a smaller invasion of privacy, the state interest in section 653aa is diminished.

Overall, the forced disclosure of an individual's full name and address in section 653aa seems to present a legally protected privacy interest and a reasonable expectation of privacy under the first and second prongs of California's privacy interest analysis. It is more questionable whether the disclosure constitutes a serious invasion of privacy under the third prong. However, since effective alternatives to the disclosure required in section 653aa invade less on an individual's right of privacy, it is possible that a court could find that the statute violates the right of privacy. This is especially likely considering that California's right of privacy is presumed to be stronger than its federal counterpart because it, unlike the federal

149. *See* Senate Judiciary Comm., Bill Analysis of S. 1506, 2003-2004 Leg., Reg. Sess., at 2 (Cal. 2004), *available at* http://leginfo.ca.gov (search 2003-2004 session for Bill Number 1506).

150. *See* Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 767-68 (N.J. Super. Ct. App. Div. 2001).

right, is explicit and because it specifically protects the individual's control over their personal information.[151]

B. Policy Concerns

1. Use of State Criminal Enforcement Resources Under California Penal Code Section 653aa

Enforcing section 653aa would require local governments to spend money and use law enforcement resources to essentially protect copyright interests, which, as discussed before, is a job exclusively left to the federal government by the Copyright Act of 1976. The fiscal effect of section 653aa involves "[p]otential non-state-reimbursable costs to local governments for enforcement, offset to some extent by fine revenues."[152] Although there is no record of any prosecutions under section 653aa, this statute has the potential of substantially burdening local law enforcement and state courts over an issue of copyright that already is covered by the federal government and its judicial and enforcement resources.[153] Federal copyright law already provides actual damages plus profits or a statutory civil penalty of up to $150,000 for every instance of willfully distributing a copyrighted work, even if it is distributed to only one person.[154] It also provides both preliminary and permanent injunctions against copyright infringement.[155] Since federal copyright law already has established substantial penalties for its violation, mirroring enforcement for what is essentially the same right might be a waste of precious local resources.

The fact that penalties for copyright violations already are severe also means that enforcement of section 653aa will not provide much of an additional deterrent effect on those who wish to infringe copyright. It is unlikely that a potential copyright infringer who is undeterred by considerable federal penalties will be persuaded into compliance by enforcement of section 653aa, especially when doing so would reveal the infringer's personal information to copyright holders and would make it easier for the infringer to be held liable under federal copyright laws. As a result, using precious government resources to enforce section 653aa would

151. Lin, *supra* note 104, at 1130.

152. Senate Judiciary Comm., Bill Analysis of S. 1506, at 2.

153. In a statement against section 653aa, the Electronic Freedom Foundation asserted that "[c]opyright law already provides for significant civil and criminal penalties. The bill will only add to the already overloaded dockets of California police, district attorneys, and courts with low-level criminal prosecutions that are, in nearly all cases, duplicative of possible federal cases." *Id.*

154. 17 U.S.C. § 504 (2006).

155. *Id.* § 502.

not only be ineffective because it merely mirrors federal enforcement efforts but also is ineffective as an additional deterrent to infringing copyright. It seems that such resources would be better spent on enforcement that more efficiently accomplishes the government's objectives.

IV. Legislative Alternatives to California Penal Code Section 653aa

California's "True Name and Address" Act has numerous legal issues surrounding it, but its troubles stem from two basic problems. First, the fact that the statute requires public disclosure of personal information from alleged infringers raises numerous privacy and obstacle preemption concerns, especially since it also requires minors to disclose their personal information. This issue is confounded by the fact that the scope of the statute goes beyond targeting just those who have infringed federal copyright law, especially in the area of fair use. Also, since subpoenas and other such methods present effective alternatives to section 653aa forced disclosure while implicating fewer privacy and preemption concerns, the reasons for allowing this disclosure become less tenable. Second, it is also clear that state law is not the proper forum for dealing with infringement of federal copyright law because of federal preemption issues.

There are two possible ways to address the state's legitimate objective of identifying copyright infringers while avoiding the problems of section 653aa. First, one could pass a law similar to the California statute, except on a federal level. This would, at the very least, remove the preemption issues. Such a statute could openly address copyright issues without running afoul of the Copyright Act. If presented as a part of federal copyright law, the statute would also instate the protections that section 653aa lacks, such as "fair use," and so would more narrowly target only those who are actually infringing upon federal copyright law. The privacy concerns inherent to forcing public disclosure of personal information would still exist, but since the federal statute would be more narrowly tailored to only target infringers under federal copyright law, it would be less likely to create an unjustified stigma on those who did not actually violate copyright law.

A second option that would avoid both the preemption and privacy concerns is devising a new method of federal subpoena. Ideally, the subpoena would allow copyright holders to protect their property rights while also installing the necessary safeguards to prevent an undue intrusion of an individual's right to privacy. The DMCA subpoena was created to

deal with just such a situation and it only became useless because of later changes in P2P technology. One solution, then, would be to create a new DMCA-style subpoena that would allow the RIAA to gain information from ISPs even when the ISP does not actually have infringing material on their servers. However, such a subpoena raises issues of the ISP's privacy concerns. When the ISP has no connection to the copyright infringement, why should it be forced to disclose its customers' information? Also, a DMCA-style subpoena requires little or no evidence of actual copyright infringement, so such a subpoena could reveal a user's private information even when the user has not violated copyright law. However, this would be better than forcing users to publicly display their information.

V. Conclusion

When the California legislature passed section 653aa, its stated intention was to make it easier for copyright holders to identify alleged copyright infringers online by circumventing the limitations of federal copyright law. This, understandably, creates numerous problems. Congress, when devising its federal law on copyright, worked carefully to balance the rights of copyright holders against the rights of other individuals. For a state to disrupt this balance by introducing their own laws on the subject, especially when the Copyright Act of 1976 explicitly forbids it, destroys the congressional goals behind the federal copyright scheme. Section 653aa's invasive disclosure requirements only further tilt this balance away from the rights of the individual. While copyright holders such as the RIAA have a right to be able to identify copyright infringers on the Internet, laws that allow this identification must be properly safeguarded and narrowly tailored to that interest to be legitimate. When, in the case of section 653aa, these concerns are ignored, the rights of the individual are in peril. Whatever laws are passed in the future to deal with these complex issues, it pays to keep these considerations in mind.

* * *