**Using Pseudonyms Online:**

 **A Legal Framework**

**Richard May**

**Santa Clara University School of Law**

**Intellectual Property Theory**

**Fall - 2014**

**I. Introduction**

This paper discusses the growing trend of using an alias or pseudonym for online activity in the Digital Age. In particular, it uses the viewpoint of an author posting written content as a means of associating different legal issues with the use of a pseudonym online. The essay first reviews the uses of a pseudonym and the trends in anonymous or undisclosed authorship online. Then the technological and social forces causing or preventing the use of aliases will be examined. Third, the essay looks to what a pseudonym-heavy society would look like, as imagined by some prominent thinkers in the area. Fourth, the legal issues surrounding the use of a pseudonym in an online context will be discussed, including the treatment of online property and written works. Last, this paper will provide suggestions for encouraging, improving, and policing use of an online alias from a legal perspective.

**II. Uses of a Pseudonym**

An online alias, often called a pseudonym, can be defined as “the use of a “virtual” personality or personalities by one physical individual when interacting in cyberspace or elsewhere.” [[1]](#footnote-1) Although the use of a fictitious online identity could be motivated by a number of factors, for authors it is often to protect one’s true identity. [[2]](#footnote-2) Reasons for an author to utilize a pseudonym online could include avoiding interference with another career, sharing a birth name with a more prominent writer, or even writing in different subject areas.[[3]](#footnote-3)

 It is difficult to determine how prevalent pseudonym use currently is online, as compared to content created under a true identity or anonymously. Using a pseudonym can prevent readers from immediately being aware of the true identity of the author, but likely will not protect someone forever.[[4]](#footnote-4) Online identities can be tied back to real life, as seen in the recent case of Michael Brutsch, a notorious reddit.com user and operating under a pseudonym that was revealed in a Gawker.com article.[[5]](#footnote-5) These instances of unmasked pseudonyms are more prevalent as technology grows, and with each outing, the national discussion of transparency and anonymity online is reopened.[[6]](#footnote-6)

 It should be noted that this essay’s discussion of anonymity, pseudonymity and transparency is in relation to privacy in an online marketplace. Anonymity in this context can be described as having two effects on an online actor; it allows the individual to hide their self-interest or any biases[[7]](#footnote-7), and it protects against repercussion or accountability outside of the online world[[8]](#footnote-8). An anonymous online market would favor privacy concerns and the generative nature of the Internet over accountability of individual users.[[9]](#footnote-9) Transparency, on the other hand, is achieved through broad and constant online surveillance, imagined with regulations in place requiring the complete public sharing of data.[[10]](#footnote-10) Proponents of either theoretical construct have legitimate arguments in their favor, but at the same time can foresee massive, dramatic shifts in the online market should one theory be put into practice.

**III. Issues with Online Aliases and Transparency**

 Often, the first thing associated with using an online alias is the prevalence of cyber-bullies and trolls. A knee-jerk reaction by many is to ban the use of anonymous writing and force writers to use real names, to promote online civility and create transparency.[[11]](#footnote-11) The argument goes that if writers and content creators are forced to use their real life identity, online defamation would dwindle.[[12]](#footnote-12) The Communications Decency Act, which became effective in 1996 and has been expanded through recent case law, can in certain instances hold Internet Service Providers liable for libelous and defamatory writing by anonymous users on their sites.[[13]](#footnote-13) This push to remove anonymity from online writing has much weight and momentum in society today.

 However, the flip side of this argument is the issue of online privacy. If every online writer were forced to use his or her true name, the amount of personal information available on any individual would grow tremendously.[[14]](#footnote-14) Imagining a truly transparent online society, issues would abound, including potential for criminal misuse and data abuse, errors in online information and profiles, and data mining concerns by commercial and governmental interests.[[15]](#footnote-15) California has already passed the Online Privacy Protection Act of 2003, which is meant to keep online users aware of privacy policies of individual Internet Service Providers.[[16]](#footnote-16) The growing technological abilities to profile online users and bombard them with behavioral targeted advertising can be equally frightening to society today.[[17]](#footnote-17) There may be solutions to privacy issues that still affect a ban on anonymity, but they likely have dire effects on freedom of speech and expression, content creation online, and even internet structure and functionality.[[18]](#footnote-18) There is a growing pull factor in society to protect personally identifiable information online and avoid full transparency of Internet content.

 This essay is focusing on the benefits of prevalence in between these two extremes; using a pseudonym is a sort of middle ground between online anonymity and perfect transparency.[[19]](#footnote-19) This essay also is viewing the rigid dichotomy of anonymity and transparency online through the lens of a legitimate content creator; rather than focus on the prevalence of trolls and cyber bullying, this essay looks at how potential regulations of online identity could affect those who are attempting to provide a benefit to society. In particular, this essay suggests ideas to protect the proliferation of individual artists, inventors and writers, as discussed in Kevin Kelly’s “1000 True Fans” theory, in which the internet provides a medium with which to make a living.[[20]](#footnote-20)

**IV. What A Pseudonym-Filled World Might Look Like**

 There have been many scholarly articles outlining, theorizing, and imagining what a society would look and feel like if pseudonyms became the prominent form of online identification. One theoretical construct is to have all online transactions completed using a limited number of “traceable” pseudonyms.[[21]](#footnote-21) The idea of traceable simply means that there is a connection between the alias and the individual, which allows two-way communication as well as the ability to conduct legal and business transactions through the pseudonym.[[22]](#footnote-22) Regulations would be needed to support this connection between the alias and the self, while maintaining limitations on the accessibility of the information indicating these connections.

 Limitations on the number of aliases allowed per individual may also need to be monitored in some way. The success of a pseudonymous society rests on the continued use of an alias for online activity by an individual.[[23]](#footnote-23) If an alias is used repeatedly, it generates a reputation, and that reputation can grow over time.[[24]](#footnote-24) This growth over time is what a pseudonymous society relies on; there is a form of accountability generated with repeated use of an alias, as the user does not want to be forced to abandon its use.[[25]](#footnote-25)

 There are social benefits to a pseudonymous society that some scholars have actually been able to observe in limited capacity in the area of social media, as well. One study found that users interacting through a secure alias were often less inhibited, and showed more intimacy and willingness to create strong personal relationships through the forum.[[26]](#footnote-26) The use of aliases for collective works is another benefit that is very tangible. Collectives such as Wikipedia, Creative Commons, and many projects within the Open Source Movement would stand to benefit from mainstream acceptance of pseudonyms online.[[27]](#footnote-27)

**V. Online Property, and Passing a Pseudonym at Death**

 There are many legal constructs that may apply to the use of a pseudonym, but there are a few in general that would be especially important for a more mainstream acceptance of aliases is found. The legal issues surrounding sale or movement of a pseudonym, the passage of a pseudonym at death, the corresponding issues of fraud and deceit, and the use of copyright surrounding aliases are all of import. This section will review the current state of the law surrounding each area.

1. **Sale of a Pseudonym, and Non-Compete Enforceability**

 It is difficult to ascertain whether a pseudonym with a good online reputation is either a good or a business unto itself. If classified and viewed as a good, standard Uniform Commercial Code rules would apply, and it is likely moveable without any special treatment.[[28]](#footnote-28) Similarly, if classified as a business, things get a little trickier, as there are tax restraints and state registration laws to comply with. Overall, it is likely that these transactions occur as a sale of goods.

 But what happens if a website operated under a pseudonym, or other online work, is sold? Would the buyer be able to enforce a non-compete agreement after the purchase? Restrictive covenants and non-competes are typically upheld only if reasonable in scope and restriction.[[29]](#footnote-29) However, in California, as well as many other states, public policy is served by disallowing most non-competes as a restraint of trade.[[30]](#footnote-30) Even if it were a reasonable, enforceable covenant, it would likely be difficult to pin down an individual writer if they operate under a pseudonym. There is likely a host of evidentiary difficulties in proving that it is the same writer if they decide to use a different alias.

1. **Passage of Online Property upon Death**

 Moving property upon death is already a tricky and sometimes difficult area of the law; when adding on that the property is digital, and further still that the “owner” may not have been the legal owner, this area becomes truly indefinable. Some federal laws that regulate the area of Internet communication and access by a fiduciary have focused on “decency” standards surrounding minors, and others regulate unauthorized access to digital accounts and assets.[[31]](#footnote-31) Both areas can constrain a fiduciary from accessing online property, whether it is banking information, emails, or online works.[[32]](#footnote-32) There are also some case law surrounding this area, and a particularly well-followed case in which a late marine’s parents fought Yahoo for access to email messages, which ultimately led to Yahoo following a probate court order and relenting on the correspondences.[[33]](#footnote-33) Ultimately, most Internet Service Providers have User Agreements that govern the accessibility and passage of user generated content to survivors; Facebook’s policy as of June 2013 was to close a user account from accessibility from any use or change once they determined the user had passed away.[[34]](#footnote-34) Many other companies simply license use of their service online to the user, with limited copyrights to the user’s content or dual ownership with restricted rights to transfer the property.

1. **Fraud and Deceit**

 The use of online aliases has long gave law enforcement officials fits, and a widespread push for pseudonym use would likely be met with a healthy dose of skepticism from those whose job it is to protect against online criminal activity. Cyber criminals, such as the perpetrators behind malware attacks, almost always operate using a pseudonym or online alias.[[35]](#footnote-35) However, the only current recourse for potential fraud or deceit online using a pseudonym relies on authorities being able to track and determine the actual identity of the user.

 Looking at these legal issues from a different perspective, if a pseudonym user was to pass their rights to the alias to another user, there would be no way of actually knowing that this occurred currently. Because of this, there would never be grounds for a fraud or deceit claim against either individual using the pseudonym. The very idea of relying on writing by a pseudonym is that you are not aware of who is actually writing. Furthermore, traditional use of a pseudonym for writing has included the works of a group or team of authors operating under a single pen name.[[36]](#footnote-36)

1. **Copyright**

If an author wishes to protect their work online through copyright law, the legal issues become a bit more defined. In the United States, an author of a copyrighted work is allowed to use a pseudonym or a pen name.[[37]](#footnote-37) Furthermore, if the author applying for the copyright does not want to identify him or herself, they simply omit their legal name on the application.[[38]](#footnote-38) Pseudonym-written works with no author identified are protected for the earlier of ninety-five years from the publication of the work or one hundred and twenty years from it’s creation.[[39]](#footnote-39) If the author’s name is given, however, standard copyright terms of life plus seventy years apply, and the author’s name is part of the public record.[[40]](#footnote-40)

**VI. Suggestions To Improve The Use of Pseudonyms**

Judith Donath is a thought leader in the area of online privacy security and the interactive world surrounding online identity, and has published a book titled “The Social Machine, Designs for Living Online.”[[41]](#footnote-41) In it she essentially argues that with pseudonyms, online actors can have the freedom to discuss or advocate on a topic that they would otherwise feel may interfere with relationships in their offline lives.[[42]](#footnote-42) However, she argues, pseudonym use would need to be anchored, possibly using “data portraits” that capture a pseudonyms history and reputation online.[[43]](#footnote-43) This anchoring would cause online actors to value reputational capital and would, in theory, reduce trolling and cyber-bullying by creating some form of accountability.[[44]](#footnote-44) Donath believes that “Pseudonyms are the most valuable contributors to [online] communities because they contribute the highest quantity and quality of comments,” and that their use encourages civility while simultaneously preserving privacy.[[45]](#footnote-45)

If pseudonym use could in fact be the happy medium between the extremes of online anonymity and transparency, then how could the legal community help its growth? Ideally, there are three areas where this essay focuses on; regulation permitting traceable pseudonym use, the ability for users to easily pass or convey online property, and the restriction of purely anonymous online content creation.

First, a regulating body would need to be formed to control and maintain the use of traceable pseudonyms. This regulating body would need to have some form of autonomy from other governmental interests, and would need to aim for protection of identity rights as its chief goal. This body would theoretically have the ability to grant pseudonym use to individuals through an application, and would need to create a mechanism to do so in which the individual's identity was able to be archived but not regularly accessible. This body would also need to implement the use of what Donath referred to as data portraits, which would need to be widely adopted by Internet Service Providers. This portrait would ultimately track and follow each pseudonym across Internet Service Providers so that accountability and continuous reputability would always be present.

Second, a handful of legislative changes would need to be enacted surrounding the passage of online assets owned or created. For example, setting up legislation that regulates the way pseudonyms (registered under the above mentioned regulating body) are transmitted between individuals. It would be important to allow individuals to pass or transmit a pseudonym with goodwill, as it is another motivational factor to encourage accountability. Furthermore, creating laws that will allow pseudonyms to be passed through testamentary rights will also encourage online civility, as individuals are reminded of how permanent the internet is, and that their actions online will live on. Other legislative changes would likely be needed, but ultimately the public policy should be to encourage pseudonym use.

The third important legal change that would need to occur in a pseudonym-filled world would be to discourage and reduce the use of pure anonymity online. This likely would not be able to be stamped out through legal means; however, encouraging Internet Service Providers to disallow anonymity on their sites would be a start. This could be accomplished through legislation that holds Internet Service Providers partially liable for tortuous acts committed on their website. A reduction in anonymity will further stimulate growth in pseudonym use in society, which further fuels the other suggestions.

**VII. Conclusion**

Overall, the idea of using a pseudonym is currently a very apt option online. However, with anonymity allowing uncivil action online, and with government action threatening individual privacy, a pseudonymous society is an appealing option. As with any dramatic societal change, there would be many unforeseen consequences following any legal shift. But a system with no accountability online, or a system with no individual privacy online, is a system that will inevitably be too extreme to maintain the Internet as we know it.

1. Zarsky, Tal Z., Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity As Overall Solutions to the Problems of Information Privacy in the Internet Society, 58 U. Miami L. Rev. 991, 1030 (2004). [↑](#footnote-ref-1)
2. Allen, Moira, Starting Your Career as a Freelance Writer, Allworth Press, 2011. [↑](#footnote-ref-2)
3. Id. [↑](#footnote-ref-3)
4. Dale, Kim Z., “Why a Pseudonym Wont Keep You Anonymous Online”, Uproarious Silence, Privacytest.com. Posted September 14, 2013. http://www.privacytest.com/blog/pseudonyms-privacy-online-anonymity/ [↑](#footnote-ref-4)
5. Chen, Adrian, “Unmasking Reddit’s Violentacrez, The Biggest Troll on the Web”, Gawker.com. Posted October 12, 2012. http://gawker.com/5950981/unmasking-reddits-violentacrez-the-biggest-troll-on-the-web [↑](#footnote-ref-5)
6. Hess, Amanda, “Gawker Outed Reddit’s Most Notorious Troll. Why Isn’t Law Enforcement Doing the Same?” Slate.com. Posted October 15, 2012. http://www.slate.com/blogs/xx\_factor/2012/10/15/reddit\_troll\_violentacrez\_outed\_by\_gawker\_when\_will\_law\_enforcement\_catch.html [↑](#footnote-ref-6)
7. Kumayama, Ken D., A Right to Pseudonymity, 51 Ariz. L. Rev. 427, 442 (2009) citing A. Michael Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases, 15 J.L. & Com. 395, 403, 409 (1996) (“[A]nonym[ity] ... makes it more difficult to identify the self interest or bias underlying an argument.... [T]he writer must be judged solely on their content as there is literally nothing else to go by.” (internal quotation marks omitted)) [↑](#footnote-ref-7)
8. Kumayama at 443. [↑](#footnote-ref-8)
9. Choi, Bryan H., The Anonymous Internet, 72 Md. L. Rev. 501, 507 (2013). [↑](#footnote-ref-9)
10. Brin, David, “The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?” page 80-84 (1998). (Conceptualising an idea of “Reciprocal Transparency”) [↑](#footnote-ref-10)
11. Donath, Judith S., “We Need Online Alter Egos Now More Than Ever” Wired.com. Posted April 25, 2014. http://www.wired.com/2014/04/why-we-need-online-alter-egos-now-more-than-ever/ [↑](#footnote-ref-11)
12. McDonald, Skyler, Defamation in the Internet Age: Why Roommates.com Isn't Enough to Change the Rules for Anonymous Gossip Websites, 62 Fla. L. Rev. 259, 262 (2010). [↑](#footnote-ref-12)
13. Id. at 266. [↑](#footnote-ref-13)
14. Donath. [↑](#footnote-ref-14)
15. Zarsky, at 1017. [↑](#footnote-ref-15)
16. Cal. Bus. & Prof. Code § 22576 (West) [↑](#footnote-ref-16)
17. Fishman, Andrea, “Privacy v. Security: What’s Behind Ad-Targeting Concern” CMO.com. Posted February 22, 2012. http://www.cmo.com/articles/2012/2/22/privacy-vs-security-whats-behind-ad-targeting-concern.html [↑](#footnote-ref-17)
18. Id. [↑](#footnote-ref-18)
19. Zarsky at 1030. [↑](#footnote-ref-19)
20. Kelly, Kevin, “1,000 True Fans” The Technium. Posted March 4, 2008. http://kk.org/thetechnium/2008/03/1000-true-fans/ [↑](#footnote-ref-20)
21. Zarsky at 1032. [↑](#footnote-ref-21)
22. Id. [↑](#footnote-ref-22)
23. Kumayama at 446. [↑](#footnote-ref-23)
24. Zarsky at 1033, discussing the idea of “reputational capital”. [↑](#footnote-ref-24)
25. Kumayama at 446. [↑](#footnote-ref-25)
26. Wellman, Barry & Milena Gulia, “Virtual Communities as Communities: Net Surfers Don't Ride Alone”, in Communities in Cyberspace, at 167, 178-81 (1997). [↑](#footnote-ref-26)
27. Kumayama at 450-51. [↑](#footnote-ref-27)
28. West's Ann. Cal. Com. Code § 2105 [↑](#footnote-ref-28)
29. Alliant Ins. Servs., Inc. v. Gaddy, 159 Cal. App. 4th 1292, 1301, 72 Cal. Rptr. 3d 259, 266 (2008). [↑](#footnote-ref-29)
30. West's Ann. Cal. Bus. & Prof. Code § 16600 [↑](#footnote-ref-30)
31. Beyer, Gerry W., JD, LLM, JSD & Naomi Cahn, JD, LLM, Digital Planning: The Future of Elder Law, NAELA, at 135, 148 (2013). [↑](#footnote-ref-31)
32. Id. [↑](#footnote-ref-32)
33. Sancya, Paul, *Yahoo Will Give Family Slain Marine's E-Mail Account*, USA Today, http://www.usatoday.com/tech/news/2005-04-21-marine-e-mail\_x.htm? POE=TEClSVA, posted Apr. 21, 2005. [↑](#footnote-ref-33)
34. Memorialization Request, Facebook <https://www.facebook.com/help/contact/651319028315841> (visited on October 19, 2014. [↑](#footnote-ref-34)
35. U.S. Attorney’s Office, “Cyber Criminal Pleads Guilty to Developing and Distributing Notorious SpyEye Malware” FBI.gov, posted January 28, 2014. http://www.fbi.gov/atlanta/press-releases/2014/cyber-criminal-pleads-guilty-to-developing-and-distributing-notorious-spyeye-malware [↑](#footnote-ref-35)
36. Allen, Moira, Starting Your Career as a Freelance Writer, Allworth Press, 2011. [↑](#footnote-ref-36)
37. U.S. Copyright Office, FL-101, “Pseudonyms”, reviewed Nov. 2010. [↑](#footnote-ref-37)
38. Id. [↑](#footnote-ref-38)
39. Id. [↑](#footnote-ref-39)
40. Id. [↑](#footnote-ref-40)
41. Donath, Judith, “The Social Machine: Designs for Living Online,” Massachusetts Institute of Technology, 2014. [↑](#footnote-ref-41)
42. Donath, Judith S., “We Need Online Alter Egos Now More Than Ever” Wired.com. Posted April 25, 2014. http://www.wired.com/2014/04/why-we-need-online-alter-egos-now-more-than-ever/ [↑](#footnote-ref-42)
43. Id. [↑](#footnote-ref-43)
44. Kumayama at 444. [↑](#footnote-ref-44)
45. Donath. [↑](#footnote-ref-45)