



1-10-2021

Social Networks, Counterfeit, and Contributory Trademark Infringement: Are Social Media Giants Still Protected Ten Years After Tiffany?

Arielle Percival

Follow this and additional works at: <https://scholarlycommons.pacific.edu/uoplawreview>

Recommended Citation

Arielle Percival, *Social Networks, Counterfeit, and Contributory Trademark Infringement: Are Social Media Giants Still Protected Ten Years After Tiffany?*, 52 U. PAC. L. REV. 877 (2021).

Available at: <https://scholarlycommons.pacific.edu/uoplawreview/vol52/iss4/12>

This Comments is brought to you for free and open access by the Journals and Law Reviews at Scholarly Commons. It has been accepted for inclusion in University of the Pacific Law Review by an authorized editor of Scholarly Commons. For more information, please contact mgibney@pacific.edu.

Social Networks, Counterfeit, and Contributory Trademark Infringement: Are Social Media Giants Still Protected Ten Years After *Tiffany*?

Arielle Percival*

I. INTRODUCTION	878
II. TRADEMARK LAW	881
A. <i>The DMCA</i>	881
B. <i>Trademark Law Foundation</i>	882
C. <i>The Connection Between Counterfeit Goods and Trademark Law</i>	883
III. SOCIAL MEDIA GROWTH AND THE RISE OF THE “COUNTERFEIT CULTURE”	884
A. <i>Development of Social Media</i>	885
B. <i>Changing Trends in Counterfeit Goods</i>	886
C. <i>Policing Counterfeits on Social Media</i>	887
IV. <i>TIFFANY (NJ) INC. v. EBAY, INC.</i> : SECOND CIRCUIT DECIDES THE FATE OF OSPs?	889
A. <i>Inwood Labs. Inc. v. Ives Labs. Inc.</i>	889
B. <i>Lockheed Martin Corp. v. Network Solutions, Inc.: Extending Inwood to Service Providers</i>	891
C. <i>Tiffany (NJ) Inc. v. eBay, Inc.: Addressing Contributory Trademark Infringement for Online Marketplaces</i>	891
1. <i>Facts and Procedural History</i>	892
2. <i>The Court’s Reasoning and Holding</i>	893
V. POST- <i>TIFFANY</i> AND BIG DATA	894
A. <i>Gaps in the Knowledge Requirement for Contributory Trademark Infringement</i>	894
B. <i>Big Data: What do OSPs Actually Know?</i>	896
VI. TRADEMARK INFRINGEMENT SAFE HARBOR	900
A. <i>The DMCA’s Safe Harbors and Their De Facto Extension to</i>	

* J.D. Candidate, University of the Pacific, McGeorge School of Law, to be conferred May 2021; B.S., Political Science, University of Oregon, 2013. First of all, I want to thank my faculty advisor, Professor Sprankling for sharing his advice and expertise with me. I would also like to thank the entire Law Review staff for their support and time spent editing this article. It truly takes a village to produce a piece of academic writing and my article is better because of it. Thank you to my family and friends for their endless love, support and encouragement. Finally, I dedicate this article to my late grandmother Eileen, an amazing woman who I try to emulate every single day through my actions and words.

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

Trademark Infringement 900
B. Europe's MoU: An Example of OSPs and IP Owners Electively
Working Together 902
VII. CONCLUSION 904

I. INTRODUCTION

One evening, Qua found what she believed was a Kylie Lip Kit on Facebook Marketplace.¹ Usually, the Kylie Lip Kit includes a lipstick and a matching lipliner.² Eager to obtain the coveted cult makeup and thinking she was receiving a good deal, Qua purchased the kit from Facebook Marketplace since it was sold out everywhere else.³ Upon receiving the kit in the mail, Qua excitedly removed the lipstick from its packaging and immediately applied the product to her lips.⁴ Moments later, Qua could not open her mouth.⁵ The lipstick superglued her lips shut.⁶ It was at this time that Qua realized she purchased a counterfeit lip kit.⁷

The sale of counterfeit items is a \$1.2 trillion industry, contributing to a \$30.3 billion loss for luxury fashion brands such as Louis Vuitton and Gucci.⁸ While brands continue to face increasing losses, the quantity of counterfeit goods entering the market continues to increase because counterfeiters no longer need to hide in the shadows or deal in back-alley transactions.⁹ E-commerce sites like Amazon and eBay, which are commonly considered marketplaces, allow counterfeit suppliers to sell their products virtually anonymously.¹⁰ However, counterfeit goods are not exclusively sold in traditional online marketplaces.¹¹ Over the last few years, counterfeiters started leveraging social media sites, like Instagram, to increase their reach to consumers.¹² A quick online search of any e-commerce or social media site reveals a range of counterfeit goods, from fake Nikes, Adidas Yeezys, and Rolex watches to more harmful items like counterfeit prescription

1. BROKEN: MAKEUP MAYHEM (Netflix 2019).
2. See KYLIE COSMETICS, <https://www.kyliecosmetics.com/> (last visited Mar. 4, 2019) (on file with the *University of the Pacific Law Review*) (selecting “lips”, then “matte lipstick kits” from the “shop” tab and finding each lip kit includes one lipstick and one lipliner).
3. BROKEN: MAKEUP MAYHEM, *supra* note 1.
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. Chavie Lieber, *Instagram Has a Counterfeit Fashion Problem*, VOX (May 2, 2019), <https://www.vox.com/the-goods/2019/5/2/18527181/instagram-counterfeit-industry-chanel-gucci-louis-vuitton> (on file with the *University of the Pacific Law Review*).
9. Lieber, *supra* note 8.
10. *Id.*
11. *Id.*
12. See *id.* (discussing counterfeit fashion accounts contributed 65 million posts to Instagram).

medication, e-cigarettes, and makeup.¹³ Counterfeit makeup is particularly harmful to consumers because of the inferior and hazardous ingredients counterfeiters use to replicate high-cost legitimate alternatives.¹⁴

The increasing sale and distribution of counterfeit products can be harmful to consumers, but it is also troublesome to the intellectual property (“IP”) owners, who own the trademarks on such products.¹⁵ As counterfeit goods flood online marketplaces, IP owners face an impossible battle of policing and regulating their marks.¹⁶ Agencies and IP owners often describe it as a “whack-a-mole” problem: when websites or IP owners remove one infringing seller, ten more “pop up” in that seller’s place.¹⁷ Additionally, an IP owner has the nearly impossible task of enforcing its rights against the direct infringer—the one that manufactures or sells the counterfeit item—since the majority of counterfeiters produce their goods in China.¹⁸

In some cases, the IP owner attempts to hold the intermediary or online service provider (“OSP”) liable under the theory of contributory trademark infringement.¹⁹ Unlike direct trademark infringement, which holds an individual liable for engaging in infringing activities, contributory trademark infringement holds a person or entity liable for encouraging or contributing to those persons that engage in infringing activity.²⁰ However, after the Second Circuit’s 2010 decision in *Tiffany (NJ) Inc. v. eBay, Inc.*, the general belief is that OSPs are not contributorily liable for their users’ direct trademark infringement unless they possess actual knowledge of specific instances of infringement.²¹

Although the reasoning from *Tiffany* remains, there is inconsistency amongst the circuits as to what information an OSP must know to satisfy the actual knowledge requirement.²² The Supreme Court had an opportunity to address the

13. BROKEN: MAKEUP MAYHEM, *supra* note 1; see Lieber, *supra* note 8 (identifying the majority of counterfeit accounts focus on selling luxury fashion knockoffs and even finding an account posted a video of counterfeit Adidas Yeezy sneakers at the manufacturing facility).

14. BROKEN: MAKEUP MAYHEM, *supra* note 1; see *Intellectual Property: CBP Can Enhance Information Sharing with the Private Sector to Address Changes in the Counterfeits Market, Testimony Before the S. Comm. on Fin.*, 115th Cong. 7–8 (2018) [hereinafter *Intellectual Property: CBP*] (statement of Kim Gianopoulos, Director, International Affairs and Trade) (noting many counterfeit goods were found to contain dangerous chemical levels and hazardous substances).

15. See *Intellectual Property: CBP*, *supra* note 14, at 2, 7 (explaining the private sector is facing increased difficulty in investigating counterfeit goods).

16. *Id.*

17. See BROKEN: MAKEUP MAYHEM, *supra* note 1 (explaining that lack of a strong punishment contributes to the problem).

18. *Intellectual Property: CBP*, *supra* note 14, at 2, 3.

19. See generally Irene Calboli, *Contributory Trademark Infringement on the Internet: Shouldn’t Intermediaries Finally Know What They Need to “Know” and “Control?”*, in RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 211, 213–20 (John A. Rothchild ed., 2016) (reviewing the evolution of the contributory trademark infringement doctrine through relevant cases).

20. *Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 854 (1982).

21. *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93 (2d Cir. 2010), *cert. denied*, 562 U.S. 1082 (2010).

22. See Calboli, *supra* note 19, at 211, 212 (claiming the courts use a “we know it when we see it” approach”).

confusion, but declined to hear this issue.²³ Since the Lanham Act does not provide requirements to hold an individual or an entity liable for contributory trademark infringement, OSPs and intermediaries are left with very little guidance.²⁴ The concepts of secondary liability and contributory infringement developed as common law doctrines, borrowing much of the reasoning from copyright cases.²⁵ Even though the Supreme Court has yet to address the issue, post-*Tiffany* cases highlight the theme that courts do not truly recognize OSPs' knowledge.²⁶ In all the cases, courts seemingly choose to ignore or not give substantial weight to the fact that when counterfeit sales occur, OSPs collect data on each listing or posting and use that data to run their businesses.²⁷

This Comment proposes that, due to advancements in technology, there is a gap in the *Tiffany* standard for finding an OSP liable for contributory trademark infringement because the data OSPs collect should raise their level of knowledge to “actual knowledge” under the current standard.²⁸ After establishing there is potential liability for OSPs under the current standard, this Comment aims to provide safety to OSPs while also addressing the enforcement needs of IP owners.²⁹ To encourage OSPs to help IP owners police their marks and protect consumers, Congress should amend the Lanham Act or enact new legislation to create a safe harbor for OSPs.³⁰ In the interim, because law often trails technology, this Comment proposes that a federal agency spearhead a private agreement between OSPs and IP owners.³¹

Part II primes the discussion of contributory trademark infringement by discussing trademark law in general.³² Part III addresses social media's growth and contribution to a counterfeit culture—highlighting the “social media influencer” sector as being particularly at risk—and provides a basic overview of the technological infrastructure that courts should consider when evaluating contributory trademark infringement cases.³³ Part IV reviews the leading case, *Tiffany v. eBay*, and its standard for determining contributory trademark

23. *Tiffany (NJ) Inc.*, 600 F.3d at 93.

24. Calboli, *supra* note 19, at 212–13.

25. *See generally id.* at 211 (reviewing the facts of each case and highlighting that each analysis relies on whether OSPs received physical notice of the infringement).

26. *See id.* at 211, 212 (claiming the courts use a “we know it when we see it” approach”).

27. *See id.* (explaining courts seem hesitant to interpret the standard too narrowly so that it will not stifle legitimate business activities); Bernard Marr, *The Amazing Ways Instagram Uses Big Data and Artificial Intelligence*, FORBES (Mar. 16, 2018, 12:28 AM), <https://www.forbes.com/sites/bernardmarr/2018/03/16/the-amazing-ways-instagram-uses-big-data-and-artificial-intelligence/> (on file with the *University of the Pacific Law Review*) (explaining how Instagram incorporates data into its decision making).

28. *Infra* Section V.B.

29. *Infra* Part VI.

30. *Infra* Parts V–VI.

31. *Infra* Section VI.B.

32. *Infra* Part II.

33. *Infra* Part III.

infringement.³⁴ Part V highlights the gap in the *Tiffany* knowledge standard and discusses why courts should place a heavier emphasis on OSPs' technology when deciding whether an OSP meets such a standard.³⁵ Finally, Part VI proposes amending the Lanham Act or enacting new legislation to include safe harbor provisions with proactive requirements for OSPs, or as an alternative to legislation in the interim, proposes a private agreement between OSPs and IP owners.³⁶

II. TRADEMARK LAW

IP is “a commercially valuable product of human intellect.”³⁷ Generally, there are four categories of IP: trademarks, copyright, patents, and trade secrets.³⁸ Article I, Section 8 of the U.S. Constitution secures the rights of copyright and patent holders by articulating Congress' right “to promote the Progress of Science and Useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”³⁹ While this Comment focuses solely on trademarks, having background knowledge of copyright law is helpful to understand the legal principles courts borrow from copyright law and apply in trademark cases.⁴⁰ Section A presents the most relevant copyright law to this Comment titled the Digital Millennium Copyright Act (“DMCA”).⁴¹ Section B provides a general background of trademark law.⁴² Section C explores how the production and sale of counterfeit goods is a violation of trademark law.⁴³

A. The DMCA

Congress enacted the DMCA in 1998.⁴⁴ As a signatory to the World Intellectual Property Organization Copyright Treaty, the U.S. needed to implement legal remedies to protect copyrighted works in the modern technological age.⁴⁵ The rise of the Internet and developments in technology allowed infringers to circumvent technological measures copyright owners used to prevent illegal

34. *Infra* Part IV.

35. *Infra* Part V.

36. *Infra* Part VI.

37. *Intellectual Property*, BLACK'S LAW DICTIONARY (11th ed. 2019).

38. PETER S. MENELL, MARK A. LEMLEY & ROBERT P. MERGES, *INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE*: 2019, at 31 (2019).

39. U.S. CONST. art. 1, § 8, cl. 8.

40. *Infra* Parts II–VI; see *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93 (2d Cir. 2010), *cert denied*, 562 U.S. 1082 (2010) (explaining the Supreme Court's observations of the *Inwood* standard in relation to a copyright case were persuasive).

41. *Infra* Section II.A.

42. *Infra* Section II.B.

43. *Infra* Section II.C.

44. 17 U.S.C.A. § 512 (West 2020).

45. GARY MYERS, *PRINCIPLES OF INTELLECTUAL PROPERTY* 149 (2017).

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

copying.⁴⁶ Internet service providers (“ISPs”) grew concerned about the foreseeable liability their companies faced by users utilizing their services to copy and distribute unauthorized works.⁴⁷ As a response to ISPs’ concerns, the DMCA created a set of safe harbors to limit “service providers” liability for infringing works.⁴⁸ The DMCA identified four kinds of ISP activity where an ISP, if in compliance with DMCA requirements, may invoke a safe harbor provision: (a) “transitory digital network communications,” (b) system caching, (c) “information residing on systems or networks at direction of users,” and (d) information location tools.⁴⁹ The third category of activity referencing information residing on networks at the direction of users establishes the notice-and-takedown (“NTD”) procedure.⁵⁰ A copyright owner uses an NTD to inform ISPs of suspected infringing material.⁵¹

B. Trademark Law Foundation

Unlike copyrights and patents which belong under the exclusive jurisdiction of the federal law, both federal and state law govern trademarks.⁵² Congress created the first federal trademark law in the late 1800s, enacting the law under the right to regulate interstate commerce.⁵³ Trademark law has continued to expand since its inception in the 1800s.⁵⁴ The Lanham Act is the main federal statute that regulates trademarks.⁵⁵ It defines a trademark as a “word, symbol, or device used by a person, or which a person has a bona fide intention to use in commerce” to distinguish his or her products and goods from others.⁵⁶ Trademarks protect consumers because they allow consumers to make informed purchases by assuring them that the products they buy are what those products purport to be.⁵⁷ On the other hand, trademarks incentivize manufacturers to produce high-quality products.⁵⁸

Trademarks also aim to create goodwill.⁵⁹ As such, trademark owners work hard to establish their mark and to build customer trust.⁶⁰ Some marks are easy to

46. *Id.*

47. MARY LAFRANCE, COPYRIGHT LAW IN A NUTSHELL 416 (2017).

48. *Id.* at 417; 17 U.S.C.A. § 512(k)(1)(A) (West 2020) (defining the term “service provider” as “a provider of online services or network access, or the operator of facilities therefor”).

49. 17 U.S.C.A. § 512(a)–(d) (West 2020).

50. *Id.* at § 512(c).

51. *Id.*

52. MENELL, LEMLEY & MERGES, *supra* note 38, at 38.

53. *Id.* at 874.

54. *See id.* (highlighting the changes to the Lanham Act throughout the years).

55. *Id.*

56. The Lanham Act, 15 U.S.C.A. § 1127 (West 2020).

57. MENELL, LEMLEY & MERGES, *supra* note 38, at 873.

58. *Id.* at 877.

59. *Id.*

60. *Id.*

recognize such as “Nike,” Nike’s “swoosh,” “Coca-Cola,” or “Tide.”⁶¹ However, even if a large population does not recognize a mark, the mark can still earn protection.⁶² Trademark owners can protect their marks so long as the mark is capable of identifying the source of the product.⁶³

Once trademark owners establish that they have a valid trademark,⁶⁴ they have the right to prevent others from using that mark.⁶⁵ In the event a person or organization unlawfully uses an owner’s mark, the Lanham Act allows a party to sue for trademark infringement.⁶⁶ If a party uses a trademark that creates a likelihood of confusion in the mind of consumers as to the source or sponsorship of the goods, that party’s use constitutes direct infringement.⁶⁷ However, over time, courts extended several secondary liability theories such as contributory liability and vicarious liability to trademarks—even though the Lanham Act does not expressly provide for such claims.⁶⁸ Contributory infringement occurs when a third party assists, induces, or continues supplying its service or product to someone it knows is directly infringing another’s mark.⁶⁹ There are other relevant theories of liability such as trademark dilution but this Comment focuses primarily on contributory infringement.⁷⁰

C. The Connection Between Counterfeit Goods and Trademark Law

Counterfeiting is a form of trademark infringement.⁷¹ A person counterfeits an item by making a copy or imitating an item without authorization and attempts to pass the copy off as the genuine product.⁷² On the spectrum of copied items, there are those that display/affix a famous trademark to an item to appear as if the item is genuine.⁷³ Alternatively, there are “dupes” or “knock-offs”—i.e., items that are similar in appearance to the genuine item but do not include the inspired item’s

61. See *Overview of Trademark Law*, BERKMAN KLEIN CTR. FOR INTERNET & SOC’Y AT HARV. U., <https://cyber.harvard.edu/metaschool/fisher/domain/tm.htm> (last visited Jan. 8, 2020) (on file with the *University of the Pacific Law Review*) (providing examples of easily recognized trademarks).

62. See *id.* (explaining the prerequisites any mark must meet to establish the mark as a trademark).

63. *Id.*

64. See *id.* (describing that a trademark owner establishes a valid trademark by proving either she was the first to register the mark with the USPTO or she used the mark first in commerce).

65. *Id.*

66. The Lanham Act, 15 U.S.C.A. § 1114 (West 2020).

67. 15 U.S.C.A. § 1114(1)(a)–(b).

68. See Calboli, *supra* note 19, at 211, 213 (summarizing the courts’ development of contributory trademark infringement through various decisions).

69. *Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 854 (1982).

70. *Infra* Parts IV–VI.

71. 15 U.S.C.A. § 1114(1)(a).

72. Arthur Zaczekiewicz, *Counterfeits, Knockoffs, Replicas: Parsing the Legal Implications*, WOMEN’S WEAR DAILY (June 2, 2016), <https://wwd.com/business-news/retail/counterfeit-knockoff-replica-legal-10437109/> (on file with the *University of the Pacific Law Review*).

73. *Id.*

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

mark.⁷⁴ Both instances of copying intend to benefit from the goodwill of the genuine items' mark; however, the sale of dupes is not always trademark infringement, while the sale of counterfeits is always trademark infringement.⁷⁵

In addition to violating trademark laws, trafficking counterfeit goods into the United States is a federal crime.⁷⁶ For repeat offenders, the law imposes a fine up to fifteen million dollars or twenty years imprisonment.⁷⁷ Additionally, at the state level, all states have some type of law addressing counterfeit goods.⁷⁸ California makes it illegal for any person who “willfully manufactures, intentionally sells, or knowingly possesses for sale any counterfeit mark.”⁷⁹ Even with the current laws in force, the sale of counterfeit goods nevertheless continues to increase.⁸⁰

III. SOCIAL MEDIA GROWTH AND THE RISE OF THE “COUNTERFEIT CULTURE”

One of the foremost contributions to increasing sales of counterfeit goods is the growth of social media.⁸¹ Social media includes “websites [or] applications that enable users to create and share content or to participate in social networking.”⁸² In 2005, only 5% of adults said they used social media.⁸³ In contrast, 72% of people today admit to using a social media site.⁸⁴ YouTube and Facebook are among the most popular.⁸⁵ In 2019, approximately seven-in-ten adults reported using Facebook, with more than half of them visiting the site daily.⁸⁶ However, younger demographics gravitate towards more image-forward sites like Instagram and Snapchat.⁸⁷ Among the eighteen to twenty-four year old demographic, approximately 75% use Instagram.⁸⁸

74. *Id.*

75. *Id.*

76. The Lanham Act, 15 U.S.C.A. § 1114(1)(a) (West 2020); 18 U.S.C.A. § 2320(a) (West 2020).

77. 18 U.S.C.A. § 2320(b)(1)(B).

78. Jeremy M. Wilson et al., *Product Counterfeiting Legislation in the United States: A Review and Assessment of Characteristics, Remedies, and Penalties*, J. Crim. L. & Criminology 521, 535 (2016).

79. CAL. PENAL CODE § 350(a) (West 2020).

80. See BROKEN: MAKEUP MAYHEM, *supra* note 1 (explaining current laws are ineffective at thwarting counterfeiting).

81. See INT'L TRADEMARK ASSOC., ADDRESSING THE SALE OF COUNTERFEITS ON THE INTERNET 8 (2017) (stating the sale of counterfeit goods on social media has “risen alarmingly”).

82. *Social Media*, LEXICO, https://www.lexico.com/definition/social_media (last visited Jan. 6, 2020) (on file with the *University of the Pacific Law Review*).

83. Brooke Auxier, Monica Anderson & Madhu Kumar, *10 Tech-Related Trends That Shaped the Decade*, PEW RES. CENT. (Dec. 20, 2019), <https://www.pewresearch.org/fact-tank/2019/12/20/10-tech-related-trends-that-shaped-the-decade/> (on file with the *University of the Pacific Law Review*).

84. *Id.*

85. Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged Since 2018*, PEW RES. CENT. (Apr. 10, 2019), <https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/> (on file with the *University of the Pacific Law Review*).

86. *Id.*

87. *Id.*

88. *Id.*

Over the last ten years, social media use has grown significantly partly because of the increase in mobile connectivity and the ease of access to smartphones.⁸⁹ In fact, only 35% of adults admitted to having a smartphone in 2011; today, approximately 81% own a smartphone.⁹⁰ Section A discusses the development of social media sites and their broadening purpose and use.⁹¹ Section B explores the changing trends in buying and selling counterfeit goods.⁹² Section C presents the problem of policing counterfeit goods on social media sites by discussing the tension between the technology, the current legal standard, and the relevant stakeholders.⁹³

A. Development of Social Media

In the beginning, social media sites like Myspace and Facebook served a more limited purpose than they do today.⁹⁴ The sites expanded upon early day social media which focused on message boards and providing people a place to communicate and share with others.⁹⁵ Today, in addition to building a network and communicating with friends, social media sites serve many purposes.⁹⁶ For example, social networks now serve as primary mediums for news, surpassing delivery by print-media in 2018.⁹⁷ Even more relevant than serving as a key medium for news is that social media has created a new industry—social media influencing.⁹⁸ Individuals are “influencers” because they influence others to purchase a product by making that product look enticing, often by wearing or using the product.⁹⁹

The influencer is replacing many traditional methods of advertisement.¹⁰⁰ Instead of a brand like Nike purchasing a TV commercial on a major television network, it will contract with an influencer to post a picture and a caption,

89. Auxier, Anderson & Kumar, *supra* note 83.

90. *Id.*

91. *Infra* Section III.A.

92. *Infra* Section III.B.

93. *Infra* Section III.C.

94. See Matthew Jones, *The Complete History of Social Media: A Timeline of the Invention of Online Networking*, HIST. COOPERATIVE (June 16, 2015), <https://historycooperative.org/the-history-of-social-media/> (on file with the *University of the Pacific Law Review*) (discussing how blogging in the early 1990s was a way for persons to express their feelings and thoughts on the Internet).

95. See *id.* (reviewing the functions of the first social media platforms).

96. See Auxier, Anderson & Kumar, *supra* note 83 (noting, as an example, that social media is used for activism).

97. Katherine Schaeffer, *U.S. Has Changed in Key Ways in the Past Decade, from Tech Use to Demographics*, PEW RES. CENT. (Dec. 20, 2019), <https://www.pewresearch.org/fact-tank/2019/12/20/key-ways-us-changed-in-past-decade/> (on file with the *University of the Pacific Law Review*).

98. Mark Goodrich & Jason Howell, *Influencers: What Every Brand and Legal Counsel Should Know*, 11 LANDSLIDE 15 (2018) (on file with the *University of the Pacific Law Review*).

99. *Id.*

100. *Id.*

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

commonly referred to as “content.”¹⁰¹ The brand benefits from this form of advertisement because by picking an influencer whose audience (i.e., the influencer’s “followers”) is within a desired demographic, the brand’s product or service reaches consumers in an authentic (because the follower trusts the influencer’s referral), more direct, and immediate manner.¹⁰²

Another channel of income for influencers is through affiliate marketing or product referrals.¹⁰³ An influencer posts content and creates links corresponding to each product.¹⁰⁴ When a person purchases the product through the link or with a specific purchase code, the influencer makes a commission.¹⁰⁵ Intermediary websites, like “liketoknow.it,” help influencers facilitate the sale of these products.¹⁰⁶ The intermediary supplies the software which creates the hyperlinks that facilitate the purchase of these goods.¹⁰⁷ Additionally, the intermediary creates a centralized location on its website for the sale of these products by directing an “influencer’s” followers to the liketoknow.it website or mobile application.¹⁰⁸ Once inside the liketoknow.it application, the user then selects the item she wants to purchase, and the intermediary redirects her to the store’s website that actually sells the product.¹⁰⁹

B. Changing Trends in Counterfeit Goods

Ever-developing technology paired with “influencer culture” is increasing the supply of and demand for counterfeit goods.¹¹⁰ Consumer behavior relating to how and where consumers buy products also contributes to increasing sales of counterfeit goods.¹¹¹ For example, in the beauty industry, new independent companies (“indie brands”) are changing the traditional distribution methods of

101. Paris Martineau, *The Wired Guide to Influencers*, WIRED (Dec. 06, 2019, 10:00 AM), <https://www.wired.com/story/what-is-an-influencer/> (on file with the *University of the Pacific Law Review*); see Goodrich & Howell, *supra* note 98 (citing a study that reported 86% of marketers use influencer marketing).

102. *Id.*; see Goodrich & Howell, *supra* note 98, at 15 (noting brands may engage with consumers more organically through influencers and that 92% of marketers found influencers to be effective).

103. *How Much Money Do Influencers Actually Make?*, MIC (Feb. 13, 2019), <https://www.mic.com/articles/192799/how-much-money-do-influencers-actually-make> (on file with the *University of the Pacific Law Review*).

104. *Id.*

105. *Id.*

106. *Influencers*, REWARD STYLE, <https://about.rewardstyle.com/> (last visited Jan. 4, 2020) (on file with the *University of the Pacific Law Review*).

107. *See id.* (explaining on its website that the company’s technology delivers a streamlined monetization solution).

108. *See id.* (allowing influencers to generate immediately shoppable content within social media platforms).

109. Dacey O’Hearn, *How Do I Purchase Items Featured on LiketoKnow.it?*, LIKETOKNOW.IT (Aug. 31, 2017) <https://help.liketoknow.it/hc/en-us/articles/115012079807-How-Do-I-Purchase-Items-Featured-on-LIKETOKNOW-it-> (on file with the *University of the Pacific Law Review*).

110. BROKEN: MAKEUP MAYHEM, *supra* note 1.

111. *Intellectual Property: CBP*, *supra* note 14, at 8.

beauty products by utilizing social media to quickly grow their companies through a direct-to-consumer (“DTC”) business model.¹¹² DTC businesses increase profit margins and speed up production timelines by interacting directly with the customer instead of utilizing an intermediary to store and sell products.¹¹³

Additionally, these indie makeup brands are experiencing rapid growth by using scarcity marketing tactics and leveraging the social media influencer culture to build excitement around their products.¹¹⁴ By launching “exclusive collections” with “limited productions,” indie brands rely on scarcity marketing tactics to generate fear in consumers that they will be unable to obtain the product in the future.¹¹⁵ Customers fear if they do not purchase the product immediately upon release, there will never be another opportunity.¹¹⁶ In some instances, people’s desire for the coveted exclusive product leads them to purchase counterfeit goods just like Qua.¹¹⁷

These social media marketing tactics are helping to grow a “counterfeit culture.”¹¹⁸ This growing “counterfeit culture” increases the demand for counterfeit goods.¹¹⁹ In some cases, the influencer unintentionally encourages others to purchase counterfeit goods by posting content including the legitimate item.¹²⁰ In other instances, influencers purposely encourage and benefit from others purchasing counterfeit goods by directly linking infringing items, oftentimes to online marketplaces like Amazon, and making a commission.¹²¹

C. Policing Counterfeits on Social Media

On the liketoknow.it app, no button exists for a user to report suspicious content, and the only reference to reporting infringing content is in the Terms of Service, which provides an email address for direct complaints.¹²² However, in the wake of *Tiffany v. eBay*, and under the belief that OSPs are liable for contributory trademark infringement only if they have “actual” knowledge, the lack of reporting mechanisms is unsurprising.¹²³ Yet the idea that social media sites do not have actual knowledge of trademark infringing items until someone reports a specific

112. BROKEN: MAKEUP MAYHEM, *supra* note 1.

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. *Id.*

118. BROKEN: MAKEUP MAYHEM, *supra* note 1.

119. *Id.*

120. *Id.*

121. *Id.*

122. *Terms of Service, LIKETOKNOW.IT* (last visited Jan. 11, 2020), <https://www.liketoknowit.com/terms-of-service/#Ownership+of+Intellectual+Property> (on file with the *University of the Pacific Law Review*).

123. *See generally* *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, 107 (2d Cir. 2010), *cert denied*, 562 U.S. 1082 (2010) (holding that more than general knowledge of infringing content is required to meet the standard).

item is confusing for one reason—data.¹²⁴

Social media sites aggregate data they collect from users' submissions and interactions for a variety of business functions, such as targeted advertising, informing preference algorithms, and improving the overall "user experience."¹²⁵ Social media sites know a user's age, name, location, what the user's face looks like, who the user has communicated with, how many times the user has logged into the application, and more.¹²⁶ A social media company knows this information by collecting and analyzing the data of each user, including but not limited to: user-submitted content, shares, likes, comments, mentions, website cookies, and metadata.¹²⁷

Metadata is "data that provide[s] information about data."¹²⁸ One of the most commonly known forms of metadata is the hashtag.¹²⁹ Hashtags connect a piece of content with a topic or theme.¹³⁰ In the counterfeit context, a seller of a counterfeit good may post a picture of the good with the hashtag of the name of the authentic good or a hashtag signaling the good is inauthentic.¹³¹ Any user who searches the same hashtag will be able to locate the posting of a counterfeit good, follow the directions the picture includes, and purchase the item.¹³² More often, the description describes these items as authentic items for resale, confusing less-savvy consumers who merely think they are receiving a bargain.¹³³

Even though it appears easy to identify sellers of counterfeit goods, the concept of hashtags underscores the primary argument of social media sites that not all users utilizing hashtags to sell items do so illegally.¹³⁴ The first-sale doctrine states that IP owners cannot enforce their rights after the initial sale of a legitimate

124. See Marr, *supra* note 27 (expressing data provides incredible "insights into human behavior").

125. See *Data Policy, Help Center*, INSTAGRAM (Nov. 1, 2017), <https://help.instagram.com/402411646841720> (on file with the *University of the Pacific Law Review*) (explaining how the data collected is used to support its products and related services); Marr, *supra* note 27 (illustrating how the large amount of data collected by social media sites is used).

126. *Data Policy, Help Center, supra* note 125.

127. Sapir Segal, *The What, Why, and How of Social Media Data*, OKTOPOST, <https://www.oktopost.com/blog/social-media-data/> (last visited Jan. 11, 2020) (on file with the *University of the Pacific Law Review*) (identifying the different types of data created by customers' engagement with content in a platform).

128. Jason Hare, *What Is Metadata and Why Is It as Important as Data Itself?*, OPENDATASOFT (Aug. 25, 2016), <https://www.opendatasoft.com/blog/2016/08/25/what-is-metadata-and-why-is-it-important-data> (on file with the *University of the Pacific Law Review*).

129. ÁGNES VESZELSZKI, *IN THE BEGINNING WAS THE IMAGE: THE OMNIPRESENCE OF PICTURES* 139 (2016).

130. *Id.*

131. See Melissa Locker, *Instagram Hashtags Feed a Thriving Black Market of Illegal Counterfeits: Report*, FAST COMPANY (Apr. 29, 2019), <https://www.fastcompany.com/90341482/instagram-hashtags-feed-a-thriving-black-market-of-illegal-counterfeits-report> (on file with the *University of the Pacific Law Review*) (reporting counterfeiters use hashtags like #MirrorQuality and #Replica).

132. See *id.* (illustrating hashtags make it easier for consumers to access and purchase counterfeit goods).

133. *Intellectual Property: CBP, supra* note 14, at 2, 3.

134. See *id.* at 2, 7 (discussing the tactics counterfeit sellers use online to appear legitimate).

good.¹³⁵ Since the first-sale doctrine protects genuine resale of goods, OSPs argue they lack the ability to discern between legitimate sellers of genuine goods and illegitimate sellers of counterfeit goods without receiving notice of a specific infringing item.¹³⁶ Therefore, according to these OSPs, they merely have “general knowledge” of infringing goods sold on their sites and are not liable under the current standard.¹³⁷

IV. *TIFFANY (NJ) INC. v. EBAY, INC.*: SECOND CIRCUIT DECIDES THE FATE OF OSPs?

Tort law provides the legal principles that comprise the common law doctrine of contributory trademark infringement.¹³⁸ *Tiffany* provides the current standard for when the law may hold an OSP liable for contributory trademark infringement.¹³⁹ Section A briefly reviews *Inwood Labs. Inc. v. Ives Labs. Inc.*, *Tiffany*'s predecessor and the last time the Supreme Court addressed contributory trademark infringement.¹⁴⁰ Section B addresses extending *Inwood* to service providers in *Lockheed Martin Corp. v. Networks Solutions, Inc.*¹⁴¹ Finally, Section C discusses the facts in *Tiffany* and the prevailing rule from the case.¹⁴²

A. *Inwood Labs. Inc. v. Ives Labs. Inc.*

The United States Supreme Court last addressed the concept of contributory trademark infringement in 1982 when it granted certiorari to a case from the Second Circuit Court of Appeals.¹⁴³ In the case, the Supreme Court considered whether generic drug manufacturers were liable for trademark infringement for manufacturing a drug with the same coloring and shape of a patented and trademark protected brand-name drug.¹⁴⁴ Ives Labs held a patent on the drug cyclandelate, which it used to treat cerebral vascular diseases and sold under the

135. See MENELL, LEMLEY & MERGES, *supra* note 38, at 1103 (explaining the defense of exhaustion/first sale to trademark infringement).

136. See *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, 98 (2d Cir. 2010), *cert denied*, 562 U.S. 1082 (2010) (claiming that eBay had limited ability to inspect goods and inexperience in determining whether the goods were counterfeit); *Intellectual Property: CBP*, *supra* note 14, at 3–7 (identifying growing e-commerce inventory and counterfeiters' new enhanced deception methods as challenges facing the private sector in policing counterfeit goods).

137. See *Tiffany (NJ) Inc.*, 600 F.3d at 107 (arguing generalized knowledge of counterfeit goods sold on their site is insufficient to meet the contributory infringement standard under *Inwood*).

138. *Id.* at 103.

139. *Id.* at 107.

140. *Infra* Section IV.A.

141. *Infra* Section IV.B.

142. *Infra* Section IV.C.

143. *Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 854 (1982).

144. *Id.* at 846.

trademark “Cyclospasmol.”¹⁴⁵ After the patent expired, generic drug manufacturers produced the drug in an identical color and shape as Cyclospasmol and marketed the drug to pharmacies as the brand-name drug equivalent.¹⁴⁶ Ives claimed that, due to the similar appearance, using look-alike capsules, and similar catalog entries, pharmacists and druggists dispensed the generic drugs—either mistakenly or purposely—as the brand-name drugs.¹⁴⁷ Further, Ives contended the generic manufacturers confused consumers by manufacturing generic drugs to look the same as the brand-name counterparts.¹⁴⁸ On appeal, the Second Circuit reversed the district court’s decision, finding the generic drug manufacturers violated § 32 of the Lanham Act.¹⁴⁹

Ultimately, the Supreme Court reversed the Second Circuit’s decision.¹⁵⁰ The Supreme Court determined the district court applied the correct standard that the law may hold a manufacturer contributorily liable for infringement when “a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement.”¹⁵¹ The standard establishes two avenues down which to show contributory trademark infringement.¹⁵² Under one avenue, a manufacturer or distributor may be liable if they induce infringement.¹⁵³ Under the other avenue, liability rests on whether the manufacturer “knows or has reason to know” of the infringement.¹⁵⁴ On appeal, the Supreme Court did not need to define the standard further; it simply found an error in the circuit court’s judgment because that court did not apply the correct standard of review.¹⁵⁵

While the majority did not further define the standard, Justice Byron White, in his concurring opinion, offered insight into what should qualify under the second “knows or has reason to know” prong.¹⁵⁶ Justice White asserted that mere anticipation of illegal substitution or believing a person *might* pass off one good for another does not create liability.¹⁵⁷ Especially in the generic drug context, Justice White explained it is important not to dilute the contributory trademark standard—which he feared the majority did—because consumers have become accustomed to generic drugs looking similar to their brand-name counterparts.¹⁵⁸

145. *Id.*

146. *Id.* at 847–48.

147. *Id.* at 850.

148. *Id.* at 849.

149. *Inwood Labs., Inc.*, 456 U.S. at 853.

150. *Id.*

151. *Id.* at 854.

152. *Id.*

153. *Id.*

154. *Id.*

155. *Inwood Labs., Inc.*, 456 U.S. at 856.

156. *Id.* at 861 (White, J., concurring).

157. *Id.*

158. *Id.* at 861–62.

B. *Lockheed Martin Corp. v. Network Solutions, Inc.: Extending Inwood to Service Providers*

Inwood articulated the rule regarding contributory trademark infringement for third parties manufacturing or distributing a product.¹⁵⁹ Seventeen years later, *Lockheed* answered the question of whether the same standard applied to service providers.¹⁶⁰ In *Lockheed*, the Court considered whether a domain name registrant, that allowed a third party to register a domain name using one of Lockheed Martin's trademarks, contributorily infringed its trademark.¹⁶¹ The defendant, Network Solutions, Inc. ("NSI"), argued it did not violate the *Inwood* standard because, as a domain name registrant, it merely offered a "service" not a "product" as *Inwood* required.¹⁶²

Recognizing the *Inwood* standard had since broadened in subsequent cases, the *Lockheed* court reconciled the rules from two cases that held lessors of flea market booth spaces liable for contributory trademark infringement if they knew or should have known their tenants sold counterfeit or copyrighted goods.¹⁶³ The court thereby concluded that *Inwood* liability applies to defendants who offer a "service" (e.g., leasing flea market spaces to tenants) if they have control over a third party's infringing activities within the service offered.¹⁶⁴

In *Lockheed*, the Ninth Circuit decided that a third-party service provider needs "[d]irect control and monitoring of the instrumentality used by a third party to infringe the plaintiff's mark."¹⁶⁵ Finding NSI was "squarely on the 'service' side of the product/service distinction," NSI did not fall under *Inwood* and its successors' contributory infringement umbrella.¹⁶⁶ Therefore, there is no liability for a service provider under *Inwood* if that service provider strictly offers a service but has no control over the medium by infringers.¹⁶⁷

C. *Tiffany (NJ) Inc. v. eBay, Inc.: Addressing Contributory Trademark Infringement for Online Marketplaces*

Equipped with the general rule from *Inwood* and the expansion of the rule from *Lockheed*, one can examine *Tiffany*, which provides the standard for contributory trademark infringement in the "modern" social media era.¹⁶⁸ Subsection 1 reviews

159. *Id.* at 854.

160. *Lockheed Martin Corp. v. Network Solutions, Inc.*, 194 F.3d 980 (9th Cir. 1999).

161. *Id.* at 983.

162. *Id.* at 984.

163. *Id.*

164. *Id.*

165. *Id.*

166. *See Lockheed Martin Corp.*, 194 F.3d at 985 (reasoning NSI is strictly on the service side because they are akin to the United States Post Service who routes the domain-name combination to the IP address).

167. *Id.*

168. *Infra* Subsections IV.C.I-II.

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

the facts and procedural history of the case.¹⁶⁹ Subsection 2 discusses the court’s reasoning and holding.¹⁷⁰

1. Facts and Procedural History

In *Tiffany*, the plaintiff, a luxury jewelry company, filed an action against eBay, Inc. in the Southern District of New York.¹⁷¹ The claim was for contributory infringement, false advertising, and trademark dilution after Tiffany discovered a large amount of counterfeit Tiffany goods for sale on eBay’s site.¹⁷² eBay, an online marketplace, gained considerable traction among the general consumer, boasting more than six million new daily listings.¹⁷³ Tiffany primarily argued that eBay was liable for contributory infringement because it knew or should have known its users sold counterfeit goods on its site and therefore satisfied the standard of liability under *Inwood*.¹⁷⁴ Further, Tiffany argued eBay profited from the counterfeit items because eBay charged each listing an “insertion fee,” a “final value fee,” and a “transaction fee” if the lister used eBay’s payment processor, PayPal.¹⁷⁵ A study estimated that eBay earned upwards of four million dollars between 2000 and 2004 from the sale of counterfeit Tiffany goods.¹⁷⁶ Tiffany submitted evidence from its investigative “Buying Programs” in 2004 and 2005, claiming that 73%–75% of all the listings on eBay selling Tiffany goods were counterfeit.¹⁷⁷ With the immediately culpable parties out of reach and as the amount of counterfeit Tiffany goods for sale on eBay continued to increase, Tiffany sought to hold eBay liable.¹⁷⁸

However, the court highlighted several actions eBay took to prevent the sale of counterfeit goods on its site, including implementing several protection policies and spending more than twenty million dollars on tools to bolster consumer trust and increase security.¹⁷⁹ eBay also created a department with over 4,000 employees whose sole purpose was combatting infringement by implementing actions such as proactively searching for blatant counterfeit listings on the site.¹⁸⁰ Most notably, eBay implemented a “notice-and-takedown system,” similar to the DMCA’s requirements, which gave IP owners a method for notifying eBay when they

169. *Infra* Subsection IV.C.I.

170. *Infra* Subsection IV.C.II.

171. *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, 96 (2d Cir. 2010), *cert denied*, 562 U.S. 1082 (2010).

172. *Id.*

173. *Id.*

174. *Id.* at 103.

175. *Id.* at 96.

176. *Id.* at 98.

177. *Tiffany (NJ) Inc.*, 600 F.3d at 96.

178. *See id.* (resolving the controversy between Tiffany and eBay, but not the perpetrators of the counterfeit activity).

179. *Id.* at 98–100.

180. *Id.* at 99.

identified infringing listings.¹⁸¹

2. The Court's Reasoning and Holding

After presenting the relevant facts, the Second Circuit first addressed Tiffany's direct infringement claim.¹⁸² Tiffany claimed eBay's use of its trademark on its website was direct infringement under § 32 of the Lanham Act.¹⁸³ The court set out a two-part test to determine if a direct trademark infringement claim exists.¹⁸⁴ First, a court determines whether a viable mark entitled to protection exists.¹⁸⁵ Second, a court considers how likely is it that the use of the mark caused consumer confusion regarding the "origin or sponsorship of the defendant's goods."¹⁸⁶ Applying the test, the court agreed with the district court's decision that eBay did not directly infringe Tiffany's mark.¹⁸⁷ The court reasoned that eBay's use of Tiffany's mark was lawful since eBay used the marks to accurately describe the sale of genuine goods on its site.¹⁸⁸

The Second Circuit next addressed Tiffany's contributory negligence claim against eBay.¹⁸⁹ After adopting *Lockheed's* extension of *Inwood* to service providers, the circuit court assumed the position that eBay as an OSP satisfied the standard because eBay exercised "sufficient control" over the counterfeit sales through its site.¹⁹⁰ The Second Circuit reiterated the *Inwood* standard that a person or organization may be liable for contributory trademark infringement if it induced another to infringe or if it "continue[d] to supply its product to one whom it knows or has reason to know is engaging in trademark infringement."¹⁹¹ Tiffany argued under the second prong of the test that eBay had "reason to know" of the infringement.¹⁹² Tiffany bolstered its argument pointing to the demand letters Tiffany sent eBay in 2003 and 2004, the findings from their Buying Programs, and the numerous Notice of Claimed Infringement forms Tiffany submitted to eBay.¹⁹³

eBay argued it had only "generalized knowledge" of the counterfeit sales and that the *Inwood* standard required more specific knowledge.¹⁹⁴ eBay supported its argument by proposing the Second Circuit recognize that the knowledge standard

181. *Id.*

182. *Id.* at 101.

183. *Tiffany (NJ) Inc.*, 600 F.3d at 101.

184. *Id.* at 102.

185. *Id.*

186. *Id.* at 103.

187. *Id.*

188. *Id.*

189. *Tiffany (NJ) Inc.*, 600 F.3d at 103.

190. *Id.* at 105.

191. *Id.* at 104.

192. *Id.* at 106.

193. *Id.*

194. *Id.* at 107, 108.

requires defendants to have knowledge of “identified individuals” infringing the product—an observation made by the Supreme Court in a subsequent copyright case applying *Inwood*.¹⁹⁵ In *Sony Corp. of America v. Universal City Studios, Inc.*, a copyright case concerning contributory infringement, the Supreme Court referred to *Inwood* as a narrow standard.¹⁹⁶ The *Sony* court required knowledge of “identified individuals” to hold a defendant liable for contributory copyright infringement.¹⁹⁷

The Second Circuit adopted eBay’s position.¹⁹⁸ In rejecting Tiffany’s proposed interpretation, the court reasoned Tiffany’s interpretation of the test was too broad and stated eBay needed “[s]ome contemporary knowledge of which particular listings are infringing or will infringe in the future.”¹⁹⁹ Applying the *Inwood* test under the narrower interpretation from *Sony* and highlighting eBay’s efforts to combat counterfeit goods, the Second Circuit held Tiffany failed to present evidence showing eBay had more than generalized knowledge of users selling counterfeit Tiffany goods.²⁰⁰

V. POST-TIFFANY AND BIG DATA

Courts generally accept *Tiffany* and *Lockheed* as the standards of “knowledge” and “control” for finding service providers liable for contributory infringement, but there is still no bright-line rule because case law of one circuit is not binding on another circuit.²⁰¹ However, it is clear that the majority of cases are very fact-specific and leave discretion for courts to decide the amount of “specific knowledge” and “control” required to hold service providers liable.²⁰² Section A compares *Tiffany* to a Ninth Circuit case where the court found a broader interpretation of knowledge permissible.²⁰³ Section B identifies the current technological capabilities of OSPs and discusses whether those capabilities should support a finding of knowledge by the OSPs.²⁰⁴

A. Gaps in the Knowledge Requirement for Contributory Trademark Infringement.

In *Louis Vuitton Malletier, S.A. v. Akonoc Solutions, Inc.* (“Akonoc”), the Ninth Circuit affirmed a district court’s jury verdict against Akonoc for

195. *Tiffany (NJ) Inc.*, 600 F.3d at 108.

196. *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 439 n.19 (1984).

197. *Id.*

198. *Tiffany (NJ) Inc.*, 600 F.3d at 107.

199. *Id.*

200. *Id.* at 109.

201. Calboli, *supra* note 19, at 224.

202. *Id.*

203. *Infra* Section V.A.

204. *Infra* Section V.B.

contributory trademark infringement.²⁰⁵ Akonoc was a web-hosting business that leased server space, Internet Protocol addresses, and provided bandwidth to websites selling counterfeit Louis Vuitton goods.²⁰⁶ The Ninth Circuit concluded a reasonable juror could find that Akonoc had actual knowledge or reason to know its clients were using its services to infringe Louis Vuitton's mark because Louis Vuitton sent Akonoc numerous notices informing it about the infringing activities.²⁰⁷ Since Akonoc was a service provider, Louis Vuitton also needed to meet the *Lockheed* test of "[d]irect control and monitoring of the instrumentality used by a third party."²⁰⁸ The Ninth Circuit, agreeing with the district court, found Akonoc had the requisite control over the third-party infringers.²⁰⁹ Analogizing Akonoc's service to a lessor of real estate, the court stated, "[a]ppellants had direct control over the 'master switch' that kept the websites online and available."²¹⁰ Thus, after *Akonoc* and *Tiffany*, OSPs like Instagram and Facebook may meet the "control" requirement since they have the "master switch" that keeps infringing profiles and listings online and can remove these profiles as easily as users create them.²¹¹

Yet the amount of "specific knowledge" required remains unclear.²¹² In *Tiffany*, the court refused to accept Tiffany's argument that the notices provided to eBay constituted sufficient knowledge.²¹³ Conversely, in *Akonoc*, the notices of infringement from Louis Vuitton were sufficient to meet the "knowledge" threshold for contributory trademark infringement.²¹⁴ Some argue the nature of the service could provide an explanation.²¹⁵ For example, if there are only a few sellers and only a few authentic products, "general knowledge" may establish contributory liability.²¹⁶ Alternatively, if there are many sellers, "knowing their identities is essential" to establish liability.²¹⁷

Additionally, what seems relevant to the analysis is whether service providers take remedial measures similar to the actions taken by eBay in *Tiffany*.²¹⁸ In *Tiffany*, eBay made a concerted effort to remove the infringing listings and implemented other corporate policies to address the problem, while the defendants

205. *Louis Vuitton Malletier, S.A. v. Akonoc Solutions, Inc.*, 658 F.3d 936, 940 (9th Cir. 2011).

206. *Id.*

207. *Id.* at 942.

208. *Id.*

209. *Id.* at 942–43.

210. *Id.* at 940.

211. *See* Calboli, *supra* note 19, at 226 (acknowledging courts are less lenient towards OSPs who failed to control their users or clearly profited from its users' infringement).

212. *Id.* at 225.

213. *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, 109 (2d Cir. 2010), *cert denied*, 562 U.S. 1082 (2010).

214. *Louis Vuitton Malletier, S.A.*, 658 F.3d at 940–41.

215. Calboli, *supra* note 19, at 224.

216. Michael Pantalony, *Contributing to Infringement: Intermediary Liability After Tiffany v. eBay and Louis Vuitton v. Akonoc*, 105 TRADEMARK REP. 709, 717 (2015).

217. *Id.*

218. *Id.* at 717–19.

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

in *Akonoc* were unresponsive.²¹⁹ However, the lack of a bright-line rule leaves uncertainty regarding how to avoid liability, resulting in varying practices amongst OSPs.²²⁰ Some OSPs have proactively implemented policies and procedures to address counterfeit items on their sites, while others—generally smaller OSPs with less resources—have yet to implement any such procedures.²²¹

B. Big Data: What do OSPs Actually Know?

Ten years post-*Tiffany*, technology has significantly progressed.²²² Data analysis and user-experience driven algorithms are the central pillars of companies within a particular category of OSPs—social media platforms.²²³ A technology company can leverage its data to eliminate spam accounts and eradicate manufactured news stories proactively; yet the belief remains that an OSP does not have “knowledge” until it receives reports of infringing material.²²⁴

OSP s have successfully argued they do not have “actual knowledge” without notice of specific infringing content despite having the necessary data.²²⁵ Despite this position, OSPs can filter and eliminate spam and hate comments without notification from users.²²⁶ Some OSPs use facial recognition to flag and suggest photos in which the user may appear to that individual user.²²⁷ The average consumer often does not know the power of data.²²⁸ But, as the power of data demystifies, a gap in the *Tiffany* standard for holding OSPs liable for contributory trademark infringement presents itself.²²⁹

Externally, the full extent of all the data points, the amount of data, or how large social media companies collect and store information will likely remain unknown.²³⁰ What these companies choose to reveal determines much of what society knows today, and what they currently disclose is subject to change at any

219. See *id.* at 720 (referencing a case where an online marketplace was held liable for contributory infringement for actively facilitating infringement).

220. Sonia K. Katyal & Leah Chan Grinvald, *Platform Law and the Brand Enterprise*, 32 BERKELEY TECH. L.J. 1135, 1164–65 (2017).

221. *Id.* at 1163.

222. See Schaeffer, *supra* note 97 (tracking the major technology trends through public surveys since 2010, the year *Tiffany* was decided).

223. Marr, *supra* note 27.

224. See generally *id.* (discussing how the social media giant uses the technology to deliver “incredible business intel and insights into human behavior”).

225. *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, 107 (2d Cir. 2010), *cert denied*, 562 U.S. 1082 (2010).

226. Marr, *supra* note 27.

227. E.g., *Data Policy, Help Center*, *supra* note 125 (explaining how Instagram uses facial recognition software).

228. See Kalev Leetaru, *How Big Is Social Media and Does It Really Count as ‘Big Data’?*, FORBES (Feb. 11, 2019), <https://www.forbes.com/sites/kalevleetaru/2019/02/11/how-big-is-social-media-and-does-it-really-count-as-big-data/> (on file with the *University of the Pacific Law Review*) (emphasizing the lack of external visibility into social media platforms’ data).

229. See generally Marr, *supra* note 27 (highlighting the powerful uses of social media data).

230. See Leetaru, *supra* note 228 (noting a lack of “external visibility” into [social media] platforms).

time at their discretion.²³¹ Additionally, the data they collect is more than what a user perceives, since the data is a combination of raw data and metadata.²³² For example, consider Twitter—a social media platform allowing users to communicate via short character-limited posts called “tweets.”²³³ When a user posts a tweet, the post creates a record.²³⁴ Just 4% of the record is the text in the tweet itself, while the remaining 96% of the record is additional data related to the tweet that the user may not observe, including how the tweet is stored.²³⁵ Understanding the extent and power of social media data is a complex endeavor.²³⁶ The lack of academic research regarding social media data highlights the tasks’ complexity while also contributing to the haze surrounding the extent of a social media company’s “knowledge”:

In recent years, the explosion of social media platforms and the public collection of social data has brought forth a growing desire and need for research capabilities in the realm of social media and social data analytics. Research on this scale, however, requires a high level of computational and data-science expertise, limiting the researchers who are capable of undertaking social media data-driven research to those with significant computational expertise or those who have access to such experts as part of their research team.²³⁷

The limited research using social media data also makes clear that a mere possession of data does not always provide a solution to individuals.²³⁸ Often, a person or computer needs to analyze the data before a company can use the data in any meaningful way.²³⁹ If data does require analysis to reveal its usefulness, then that requirement supports the OSPs’ argument that they only have generalized knowledge because they do not necessarily have a particular data record of

231. *See id.* (commenting that the information we know about social media companies is information these companies choose to provide); *Platform Policy*, INSTAGRAM, <https://www.instagram.com/about/legal/terms/api/> (last visited Mar. 5, 2020) (on file with the *University of the Pacific Law Review*) (“We reserve the right to change this policy at any time without notice, so please check it regularly.”).

232. Leetaru, *supra* note 228.

233. *Id.*

234. *Id.*

235. *Id.*

236. Joseph T. Yun et al., *The Social Media Macroscopic: A Science Gateway for Research Using Social Media Data*, 111 FUTURE GENERATION COMPUTER SYS. 819, 819 (2019) (on file with the *University of the Pacific Law Review*).

237. *Id.*

238. *See Harness the Power of Big Data for a New Economy*, IBM BIG DATA & ANALYTICS HUB, <https://www.ibmdatahub.com/infographic/harness-power-big-data-new-economy> (last visited Mar. 4, 2020) (on file with the *University of the Pacific Law Review*) (providing an infographic that describes how to leverage data through analytics).

239. *See Segal, supra* note 127 (depicting data as the “raw ingredients” and analytics as the “recipe” need to produce insightful information).

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

counterfeit goods.²⁴⁰ This concept of “having” versus “knowing” aligns with other areas of law as well that distinguish possession of information from knowledge of information.²⁴¹

On the other hand, OSPs analyze countless amounts of data to inform and run their businesses.²⁴² Some ways OSPs use the data is by evaluating user behavior within the application to determine how the applications present ads to each user, performing internal research for future business and technical development, personalizing their product offerings, and more.²⁴³ Thus far, OSPs have hid behind a veil of ignorance.²⁴⁴ However, because OSPs already use data which could identify counterfeit sellers (e.g., location, behavior, Internet Protocol address of the specific user, etc.) to make internal business decisions, and since those business decisions are made by an employee within the company, OSPs should meet the knowledge requirement for contributory trademark infringement.²⁴⁵

Although the technology likely exists for OSPs to easily and quickly identify and eradicate counterfeit items from their websites and applications, the central question is what liability the law *should* impose on an OSP versus what liability it *can* impose on OSPs.²⁴⁶ An OSP would argue it has no affirmative duty to investigate and police trademark infringing items.²⁴⁷ The duty to enforce one’s mark lies with the owner of the mark.²⁴⁸ Also, OSPs argue that they are unable to decipher the difference between counterfeit listings or postings and legitimate, non-infringing postings.²⁴⁹ If one accepts that OSPs cannot accurately differentiate between legitimate and non-legitimate content unless the IP owner specifically identifies infringement, then requiring OSPs to take a more proactive role in eradicating counterfeit will require technological development.²⁵⁰

Writing the code to perform actions within an application is not a free endeavor; all technological developments come with a cost.²⁵¹ To illustrate,

240. See generally *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93 (2d Cir. 2010), *cert denied*, 562 U.S. 1082 (2010) (arguing that generalized knowledge is insufficient to impose a burden on an OSP).

241. See CAL. PENAL CODE § 496 (West 2020) (requiring for the crime of larceny that the person knowingly possesses stolen property).

242. See *Data Policy, Help Center*, *supra* note 125 (describing how Instagram employs user data).

243. *Id.*

244. DANNY FRIEDMANN, *TRADEMARKS AND SOCIAL MEDIA* 268 (2015).

245. *Id.*

246. *Id.* at 254, 260.

247. STAFF OF S. FIN. COMM., 116TH CONG., *THE FIGHT AGAINST FAKES: HOW STATUTORY AND REGULATORY BARRIERS PREVENT THE SHARING OF INFORMATION ON COUNTERFEITS* app. B, Consumer Technology Association letter, at 4 (Comm. Print 2019).

248. FRIEDMANN, *supra* note 244, at 255.

249. *Intellectual Property: CBP*, *supra* note 14, at 2, 7.

250. See FRIEDMANN, *supra* note 244, at 264 (challenging the Court of Justice of the European Union’s decision that requiring proactive filtering would be too costly for the OSP).

251. See Matt Weinberger, *Pinterest Has Spent \$309 Million on Amazon’s Cloud Since 2017 as Part of a \$750 Million Contract*, BUS. INSIDER (Mar. 22, 2019, 2:28 PM) <https://www.businessinsider.com/pinterest-ipo-amazon-web-services-2019-3> (on file with the *University of the Pacific Law Review*) (detailing the cost Pinterest will spend on server space).

Business Insider reported that Pinterest, a social media site dedicated to sharing photo-forward content, will spend \$750 million on Amazon Web Services (“AWS”) between May 2017 and July 2023.²⁵² AWS is a cloud-based server system that many social media sites like Pinterest—and at one time Instagram—use to host most of the website’s software and applications.²⁵³ Before switching to Facebook’s server center, Instagram—also a photo-focused social media site—used thousands of machines at AWS to run its application.²⁵⁴ Considering Instagram has a higher number of users than Pinterest, with one billion active users as of January 2020 compared to Pinterest’s 322 million active users, the cost to run an application like Instagram and store its data is far greater.²⁵⁵ Also, not all the costs are solely monetary.²⁵⁶ Every time a website implements a new feature or runs a new data query, the developer must ensure the update does not adversely impact the website’s overall performance or a user’s experience.²⁵⁷

An IP owner would argue that because of OSPs’ infrastructure, they must take a more proactive position in combatting the sale of counterfeit goods.²⁵⁸ OSPs have direct control over the infringing content and can “pull the plug” on the listings anytime.²⁵⁹ From a moral perspective, since OSPs benefit financially—at least indirectly by incorporating counterfeit sellers’ user data into their business decisions and directly through potential ad sales—OSPs should actively monitor for counterfeit listings.²⁶⁰ Additionally, as the source of the data, OSPs are in a better position than third parties to identify efficient and effective methods to pinpoint counterfeit goods.²⁶¹

The dichotomous wishes of these two constituents, IP owners and OSPs, led to the DMCA’s safe harbor provisions.²⁶² The goal was to offer protection for OSPs and to ensure the internet continued to improve, while at the same time addressing the concern of copyright holders due to the sudden increase of

252. *Id.*

253. *Id.*

254. See Cade Metz, *How Facebook Moved 20 Billion Instagram Photos Without You Noticing*, WIRED (June 26, 2014), <https://www.wired.com/2014/06/facebook-instagram/> (on file with the *University of the Pacific Law Review*) (explaining the heavy task of Instagram’s server migration to Facebook servers).

255. See *Most Popular Social Networks Worldwide as of January 2020, Ranked by Number of Active Users*, STATISTA (Feb. 14, 2020), <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (on file with the *University of the Pacific Law Review*) (discussing client bases for both companies).

256. See Metz, *supra* note 254 (discussing how the server migration could not be a disruption for its users).

257. See Interview with Earl Damron, Director of Software Engineering, SkySlope, in Sacramento, Cal. (Feb. 3, 2018) (notes on file with the *University of the Pacific Law Review*) (identifying time and security risks as two considerations engineers must consider when developing and implementing new technology).

258. See FRIEDMANN, *supra* note 244, at 266 (proposing OSPs are in a better position to monitor for counterfeit goods on their sites because the content “falls within their control”).

259. *Id.*

260. *Id.* at 252, 266.

261. *Id.* at 267.

262. Edward J. Damich, *Commentary: The Digital Millennium Copyright Act*, in 4 INT’L INTELL. PROP. L. & POL’Y 80-1 to -2 (Hugh C. Hansen ed., 2000).

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

copyright infringement online.²⁶³ However, unlike copyright protection, trademarks act as a form of consumer protection, and thus it is even more necessary to enact similar legislation.²⁶⁴

VI. TRADEMARK INFRINGEMENT SAFE HARBOR

This Comment suggests a proactive approach to addressing the increase in counterfeit goods available on the market.²⁶⁵ Enacting legislation similar to the DMCA, which created a safe harbor for OSPs for copyright infringement, is the first step in providing clarity surrounding contributory liability for OSPs and IP owners.²⁶⁶ However, a direct replica of the DMCA's safe harbor provisions does not best combat the problem, so the legislation should include a few proactive requirements for OSPs.²⁶⁷ Section A discusses the DMCA provisions that the trademark infringement safe harbor should incorporate.²⁶⁸ Section B follows with a discussion of the European Union's Memorandum of Understanding ("MoU") between Internet Platforms and Rights Owners and why it is a valid solution to the counterfeit problem in the interim.²⁶⁹

A. The DMCA's Safe Harbors and Their De Facto Extension to Trademark Infringement

Congress should enact a trademark infringement safe harbor for OSPs similar to the DMCA.²⁷⁰ The DMCA provides a safe harbor from secondary liability for copyright infringement if an OSP meets specific requirements.²⁷¹ Primarily, an OSP is immune from secondary liability for copyright infringement if it does not have constructive knowledge or actual knowledge of the infringing material.²⁷² Even if the OSP obtains the required knowledge, an OSP is still immune from liability if it acts quickly to remove or prevent access to the content.²⁷³ However, the DMCA only shields an OSP from liability if the OSP complies with the NTD procedures stated in the DMCA.²⁷⁴

263. *Id.* at 80-2.

264. MENELL, LEMLEY & MERGES, *supra* note 38, at 873.

265. *Infra* Part VI.

266. *Contra* FRIEDMANN, *supra* note 244, at 270 (taking the opposing view that legislature should not enact safe harbors for OSPs).

267. *See id.* at 253 (highlighting safe harbor provisions like those in the DMCA have a passive effect on social media companies and encourage them to act only reactively, leading to a "flood of legal conflicts").

268. *Infra* Section VI.A.

269. *Infra* Section VI.B.

270. *See* Calboli, *supra* note 19, at 211, 230 (arguing Congress should adopt safe harbor provisions modeling after the DMCA).

271. 17 U.S.C.A. § 512(c)(3)(A) (West 2020).

272. FRIEDMANN, *supra* note 244, at 226.

273. *Id.*

274. 17 U.S.C.A. § 512(c)(1)(A)(iii).

The DMCA sets the standard for how OSPs address copyrighted material on their websites, but the statute is not applicable to trademark infringement; it applies only to copyright infringement.²⁷⁵ Even so, in the case of trademark infringement, the DMCA has “set a de facto standard in regard to notice and takedown procedures.”²⁷⁶ As such, most large OSPs utilize the same procedure for removing or disabling access to trademark infringing content or goods.²⁷⁷ Since OSPs are familiar with the DMCA’s NTD requirements, it would be efficient to implement a system for trademark infringement removal requests that the OSPs are comfortable with and currently use.²⁷⁸

Like the DMCA, the trademark infringement safe harbor should require an OSP to implement NTD procedures to be free from liability.²⁷⁹ Responses to NTD requests should be within a reasonable time, taking into consideration the size and business model of the OSP.²⁸⁰ For example, a larger OSP like Instagram could reasonably respond to a request within twenty-four hours, while a small company with three employees may deserve more leeway.²⁸¹ Additionally, to assist IP owners in enforcing their rights on the sites, the law should require OSPs to provide appropriate reporting to IP owners who register with the OSP and who provide the OSP with a list of keywords and search terms that the OSPs can use to easily run a report.²⁸² An example of a compliant program is Amazon Brand Registry, which provides IP owners additional protective measures to enforce their marks on Amazon.²⁸³

In proposing that each company implement a program similar to Amazon Brand Registry, the trademark infringement safe harbor contradicts the DMCA.²⁸⁴ Section 512 of the DMCA prescribes that no substantial burden or cost should be placed on OSPs that would hinder the administration of their network and systems.²⁸⁵ Within the realm of copyright, where infringing material does not pose

275. FRIEDMANN, *supra* note 244, at 225.

276. *Id.* at 229.

277. *Id.*

278. *See id.* at 230 (stating OSPs have implemented DMCA-style NTD procedures for trademark holders).

279. *See* European Commission, Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet, at 4 (June 21, 2016), https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en (on file with the *University of the Pacific Law Review*) (expressing NTDs are indispensable).

280. *See* Locker, *supra* note 131 (providing a statement from an Instagram representative explaining the company responds to most NTD requests within one day).

281. *Id.*; *see also* European Commission, *supra* note 279, at 5 (committing OSPs to take proactive steps that are commercially and technically reasonable given the provider’s business model).

282. European Commission, *supra* note 279, at 4.

283. *See Benefits of Amazon Brand Registry and Protection*, AMAZON, <http://brandservices.amazon.com/benefits> (last visited June 7, 2020) (on file with the *University of the Pacific Law Review*) (describing the benefits of the programs to brands who register including additional security protections for infringing content).

284. *See* FRIEDMANN, *supra* note 244, at 264 (noting the DMCA prohibits technical standards from imposing substantial costs).

285. 17 U.S.C.A. § 512(i)(2)(c) (West 2020).

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

a potential health and safety risk to consumers, prescribing that the NTD requirements should not significantly burden the OSPs is justified.²⁸⁶ Yet in light of the risks posed to consumers especially in relation to counterfeit goods, imposing more burden on OSPs for trademark infringement NTDs is also justified.²⁸⁷ Furthermore, even if requiring all OSPs to develop or implement a program similar to Amazon Brand Registry involves technical costs for the OSPs, the cost is likely far less than an alternative solution requiring complete proactive filtering on the part of the OSP.²⁸⁸

With this solution, the OSP is presenting the information to the IP owners.²⁸⁹ However, the responsibility remains with the IP owner to police its mark because the owner still must flag the material (i.e., provide notice to the OSP) for removal.²⁹⁰ Additionally, if OSPs only must analyze a data set limited to the keywords and images provided by the IP owners, then the query is less demanding on the OSPs' networks than a complete search of all their data.²⁹¹ In conclusion, the trademark infringement safe harbor borrows the NTD procedures from the DMCA but implements an additional proactive requirement where OSPs better assist IP owners in monitoring their mark.²⁹²

B. Europe's MoU: An Example of OSPs and IP Owners Electively Working Together

Congress should amend the Lanham Act or enact new legislation because a statute provides the most clarity for how OSPs and IP owners are to proceed.²⁹³ Additionally, while the *Tiffany* rule provides direction from the courts, the rule does not necessarily incorporate the beliefs and preferences of all stakeholders like the legislative political process does.²⁹⁴ However, it is well known that the law

286. See FRIEDMANN, *supra* note 244, at 265 (suggesting OSP's cost concerns are fictitious).

287. See *Intellectual Property: CBP*, *supra* note 14, at 7 (explaining some counterfeit goods pose serious health risks).

288. See FRIEDMANN, *supra* note 244, at 265, 303 (proposing to eliminate safe harbors and requiring OSPs implement a proactive system that will lead to "algorithmic justice").

289. Cf. *Benefits of Amazon Brand Registry and Protection*, *supra* note 283 (proclaiming the Brand Registry provides a proactive approach).

290. Cf. *id.* (noting the Brand Registry requires brands to submit a report after completing a search for infringing material).

291. Interview with Earl Damron, *supra* note 257.

292. 17 U.S.C.A. § 512(c) (West 2020); see also STAFF OF S. FIN. COMM., 116TH CONG., THE FIGHT AGAINST FAKES: HOW STATUTORY AND REGULATORY BARRIERS PREVENT THE SHARING OF INFORMATION ON COUNTERFEITS app. B, Consumer Technology Association letter, at 4 (Comm. Print 2019) (noting "the 60,000 brands already enrolled in [Amazon Brand Registry] are finding and reporting 99% fewer suspected infringements than before its launch").

293. See Interview with Eleanor Lackman, Partner, Mitchell Silberberg & Knupp LLP SkySlope (Apr. 7, 2020) (notes on file with the *University of the Pacific Law Review*) (commenting that while the courts often do a god job interpreting the standard, the legislative process is likely a better way to proceed in new areas of law because it allows for stakeholder involvement).

294. See generally STAFF OF S. FIN. COMM., 116TH CONG., THE FIGHT AGAINST FAKES: HOW STATUTORY

often trails advancements in technology, so amending the Lanham Act may take time.²⁹⁵ Therefore, a solution encouraging private cooperation between OSPs and IP owners provides an interim solution for the problem.²⁹⁶

In Europe, OSPs and IP owner constituents voluntarily submitted to private company cooperation to combat the sale of counterfeit goods on the Internet.²⁹⁷ The Commission to the European Parliament facilitated the agreement and encouraged dialogue between stakeholders.²⁹⁸ First signed in 2011, the Commission describes the European Union's MoU as an industry-led initiative, with companies such as Facebook and Hermès signing on as recent as October 2018.²⁹⁹ Stakeholders view the MoU as successful, emphasizing that the agreement encourages discussion between key stakeholders.³⁰⁰ However, IP owners still seek more transparency from the OSP participants, calling for the Internet Protocol addresses, phone numbers, emails, and even bank account details of specific offenders.³⁰¹ This urging for more information reveals that even in a completely voluntary setting, OSPs actively protect their data.³⁰² The lack of a compulsory requirement for OSPs to provide relevant data to IP owners is one reason why a regulated safe harbor provision better addresses the problem.³⁰³ On the other hand, the signatories recognize that NTDs do not best address the sale of counterfeit goods over the Internet.³⁰⁴ If NTDs are not the best solution to address the problem, then it raises the question whether a safe harbor similar to the DMCA is the best path forward.³⁰⁵ Regardless, one positive outlook from OSPs is that they believe the "efficiency of cooperation and bilateral relations" will continue to grow as

AND REGULATORY BARRIERS PREVENT THE SHARING OF INFORMATION ON COUNTERFEITS 32 (Comm. Print 2019) (affixing to its report letters from right holders and e-commerce platforms).

295. See Press Release, House Comm. on the Judiciary, Nadler, Collins, Johnson & Roby Introduce Bipartisan SHOP SAFE ACT to Protect Consumers and Businesses from the Sale of Dangerous Counterfeit Products Online (Mar. 2, 2020) (on file with the *University of the Pacific Law Review*) (calling for legislation because "the current legal regime does not adequately incentivize online platforms to vet who is selling on their website and what they are selling").

296. See STAFF OF S. FIN. COMM., 116TH CONG., THE FIGHT AGAINST FAKES: HOW STATUTORY AND REGULATORY BARRIERS PREVENT THE SHARING OF INFORMATION ON COUNTERFEITS 5 (Comm. Print 2019) (including Senator Wyden's statement noting that the federal government's responsibility for ensuring their approach to counterfeit is not "stuck in the 20th century").

297. European Commission, *supra* note 279, at 4.

298. European Commission, *Overview of the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet*, at 1, COM (2017) 707 final (Nov. 29, 2017), <https://ec.europa.eu/docsroom/documents/26602> (on file with the *University of the Pacific Law Review*).

299. *Industry-led Initiative to Fight Counterfeiting Gets New Boost*, EUR. COMMISSION (Jan. 3, 2019), https://ec.europa.eu/growth/content/industry-led-initiative-fight-counterfeiting-gets-new-boost_en (on file with the *University of the Pacific Law Review*).

300. European Commission, *supra* note 298, at 1, 11.

301. See *id.* at 1, 13 (noting all IP owners call for more transparency in the data, stressing aggregated data is not useful for enforcement of rights).

302. *Id.* at 1, 13.

303. But see *id.* at 1 (stressing voluntary agreements can be successful and provides flexibility).

304. *Id.* at 1, 6.

305. See *id.* at 1 (recognizing a voluntary approach to combat the sale of counterfeit goods can be effective).

2021 / Are Social Media Giants Still Protected Ten Years After Tiffany?

OSPs and IP owners work together and establish methods for preventing the sale of counterfeit goods.³⁰⁶

VII. CONCLUSION

While many believe *Tiffany v. eBay* foreclosed the discussion on whether an OSP can be liable for contributory trademark infringement, advancements in technology show a weakness in the consensus that most OSPs only have generalized knowledge of the infringing content on their sites.³⁰⁷ The amount of data OSPs collect and use to make informed business decisions creates an inference that—at the very least—OSPs have actual knowledge of infringement on their sites.³⁰⁸ While it remains unclear whether OSPs can be held liable for contributory trademark infringement under the current standard, it is clear that both OSPs and IP owners agree that the sale of counterfeit goods is a real problem.³⁰⁹ Although OSPs have access to a wealth of information, they are not the actual infringers.³¹⁰ Thus, the solution must take into consideration IP owners desire to protect their rights without overly burdening OSPs.³¹¹ Cooperation between these two stakeholders is necessary to address the increased sales of counterfeit goods online.³¹² Since there are no current regulations to encourage cooperation, the hope is that Congress will amend the Lanham Act to enact safe harbor provisions for OSPs that also provide new enforcement tools for IP owners.³¹³

306. European Commission, *supra* note 298, at 1, 10.

307. *See generally* Calboli, *supra* note 19, at 224 (describing the lack of certainty surrounding OSPs required degree of “knowledge”).

308. *See Data Policy, Help Center, supra* note 125 (describing how Instagram employs user data).

309. *See* STAFF OF S. FIN. COMM., 116TH CONG., THE FIGHT AGAINST FAKES: HOW STATUTORY AND REGULATORY BARRIERS PREVENT THE SHARING OF INFORMATION ON COUNTERFEITS 9–10 (Comm. Print 2019) (indicating diverse industries believe more reliable data is key to fighting the sale of counterfeit).

310. *See generally* FRIEDMANN, *supra* note 244, at 249, 265 (explaining the technological capabilities of OSPs and the difficulties IP right holders face holding direct infringers accountable compared to OSPs).

311. *See* STAFF OF S. FIN. COMM., 116TH CONG., THE FIGHT AGAINST FAKES: HOW STATUTORY AND REGULATORY BARRIERS PREVENT THE SHARING OF INFORMATION ON COUNTERFEITS 6 (Comm. Print 2019) (confirming e-commerce sites have no affirmative duty to police the sale of counterfeit on its sites).

312. *See generally* European Commission, *supra* note 298, at 1 (recognizing collaboration between key stakeholders is integral to prevent the online sales of counterfeit goods).

313. *See* Shop Safe Act of 2020, H.R. 6058, 116th Cong. § 2 (2020) (introducing legislation in March 2020 addressing contributory liability for OSPs in connection with counterfeit goods that implicate serious health and safety concerns).