Spring 2013

INTELLECTUAL PROPERTY LEGAL DEVELOPMENTS 2011-2012: THE YEAR IN REVIEW

Peter Brown

Richard Raysman

INTELLECTUAL PROPERTY LEGAL DEVELOPMENTS 2011-2012: THE YEAR IN REVIEW

*Peter Brown**
*Richard Raysman***

I. INTRODUCTION

The Internet has become an indispensable tool, one that has become an integral part of our lives. It is utilized in almost every aspect of daily life: to gather information, to conduct financial transactions, to communicate through social networks, and to sell or purchase items. However, along with the Internet's obvious benefits, it also presents unique issues and has resulted in new and unexplored territory for those in the legal field. For example, online retailers collect, store, and share consumer information, sometimes without the consumer's knowledge. The ability to easily create and use websites may allow online retailers to more easily sell counterfeit goods, sometimes without the consumer having any knowledge.

This article will address several legal issues pertaining to the Internet. Recent developments in online behavioral advertising and data collection will be addressed, followed by a discussion of contributory online trademark infringement in relation to the sale of counterfeit goods. Both are issues whose extent of risk and impact are not fully understood, are still being explored, and are not clear-cut.

First, the authors explore what is known as behavioral or targeted advertising; advertising that is tailored to each consumer.[1] Typically, consumers are unaware that their online activities are being tracked in this manner, since most sites do not collect personal information (e.g., a consumer's name or address), but instead track a consumer through the use of cookies.[2] While contextual advertising, or what seems to be the more traditional form of advertising, is simply random advertisements popping up on someone's Internet browser, behavioral advertising gives companies the ability to track a consumer's online behavior and target advertisements toward that individual consumer.[3] This form of advertising can be beneficial to both the advertiser and the consumer, but some inherent privacy risks exist with this practice and raise valid concerns on the part of the consumer.[4]

The discussion explores online data collection, and considers the legal steps taken to regulate this form of advertising. Potential issues involved with the practice of sharing consumers'

---

* Partner, Baker & Hostetler LLP. B.A., Dartmouth College (1968); J.D., Columbia University School of Law (1972).

** Partner, Holland & Knight LLP. B.S., MIT (1968); J.D., Brooklyn Law School (1973).

[1] KATHLEEN ANN RUANE, CONG. RESEARCH SERV., RL 34693, PRIVACY LAW AND ONLINE ADVERTISING: LEGAL ANALYSIS OF DATA GATHERING BY ONLINE ADVERTISERS SUCH AS DOUBLE CLICK AND NEBUAD 1 (2008).

[2] *See* Yoriko Matsuda et al., *Data Collection: Defining the Customer*, DIRECT MARKETING ON THE INTERNET, http://web.mit.edu/ecom/www/Project98/G2/data.htm. *See* Scott Killingsworth, *Website Privacy Policies In Principle and In Practice*, 618 PRACTISING L. INST.: PATS., COPYRIGHTS, TRADEMARKS, & LITERARY PROP. COURSE HANDBOOK SERIES NO. G0-00DZ 667, 672, 726 (2000).

[3] Ruane, *supra* note 1.

[4] *See id.* at 1, 12.

information with third parties are discussed, along with the regulations evolving in an attempt to address the issue. As the authors discuss, advertisements are also appearing on smartphones, and alleged misuses have resulted in lawsuits. Last, the article discusses whether the online marketing industry's self-regulation will meet the needs of the Federal Trade Commission (FTC) and Congress.

II. ROLE OF THE INTERNET IN SALES AND MARKETING

Online retailers and others are using new technologies to collect, store, manipulate, and share ever-increasing amounts of consumer data at very little cost. The latest techniques in online targeted advertising depend upon capturing consumer web browsing, social media, and location-based mobile service data over time. However, recently the ease with which companies collect and combine online information from consumers has raised some concerns about consumer privacy. Some consumers are troubled by the sharing of their information or compiling of comprehensive profiles, others have no idea that it is taking place, and still others may be aware of such online data collection but view it as a worthwhile tradeoff for innovative products and convenience.

This article will discuss the current legal landscape surrounding online behavioral advertising and data tracking, including recent actions by the marketing industry and Federal Trade Commission (FTC) and the latest developments surrounding geolocation and the development of a Do Not Track web browsing mechanism.

A. *Behavioral Advertising Generally*

Generally speaking, behavioral advertising is the tracking of a consumer's online activities (e.g., search engines queried, web pages visited, e-commerce activities) to deliver advertising targeted to that individual consumer's interests. The practice, which is typically invisible to consumers, allows businesses to align their ads more closely to the inferred interests of their audience.[5] In many cases, the information collected is not personally identifiable in the traditional sense and is "anonymized" by the data collectors – that is, the information does not include the consumer's name, physical address, or similar identifier that could be readily used to identify the consumer in the offline world.[6]

Online data collection can be either active or passive. Active data collection requires a user to deliberately share personal data, such as completing an online purchase or survey.[7] Passive data collection, on the other hand, includes capturing user preferences and usage behavior without consumer interaction, such as the placing of "cookies" on a user's computer or mobile device that contain unique identifiers and browsing history information to track a user's online movements.[8] Generally speaking, a cookie is a small text file that a website's server places on a computer's Web browser. The cookie transmits information back to the website's server about the user's browsing activities on the site, including pages viewed, the time and duration of visits, search engine queries, and whether an online advertisement was clicked on.[9]

---

[5] Ruane, *supra* note 1.

[6] Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, at A1.

[7] *See supra* note 2.

[8] *Id.*

[9] Tech Target: Software Quality, *Definition: Cookie*, http://searchsoftwarequality.techtarget.com/definition/cookie.

The sharing of this collected data among third parties is poorly understood by individuals and is not necessarily communicated transparently to users by many websites and applications. When a user visits a website, beyond the site's own first-party advertising cookies, the site might also insert third-party advertising network cookies onto the user's computing device containing a unique ID number.[10] Some websites (e.g. Wikipedia) do not place any tracking cookies,[11] while other high-traffic sites place multiple cookies onto a user's computer that transmit details about their visitors to outside network advertisers.[12] The practice of placing ordinary browser cookies has been upheld by courts, and in one notable case, a federal district court held that website visitors do not suffer a cognizable "economic loss" from the collection of their data.[13] Ordinarily, computer users can delete browser cookies by using tools within their Web browser to prevent third parties from associating the user's browsing history information with their subsequent web activity.[14]

However, some entities have purportedly sidestepped consumer choices regarding behavioral advertising through certain technological techniques, such as using supercookies (or "Flash cookies") which "respawn" browser cookies in a different location without notice to or consent of the user.[15] The practice has prompted numerous civil actions.[16] The placing of supercookies has also resulted in enforcement actions.[17]

Once a Web user's browsing data is collected and stored in a browser cookie, it can be aggregated by third party firms, or network advertisers that select and deliver advertisements across the Internet on websites that participate in their networks. In subsequent web surfing sessions, if a user visits websites that are served by the same advertising network, the networks can analyze the

---

[10] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., Jul. 30, 2010, *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[11] *What They Know: Wikipedia.org Privacy Policy & Online Tracking Data*, WALL ST. J. (Jul. 30, 2010), http://blogs.wsj.com/wtk/2010/07/30/wikipediaorg/.

[12] *See What They Know: YouTube.com Privacy Policy & Online Tracking Data*, WALL ST. J. (Jul. 30, 2010), http://blogs.wsj.com/wtk/2010/07/30/youtubecom/. *See also What They Know*, WALL ST. J. (Jul. 30, 2010), http://blogs.wsj.com/wtk/.

[13] *See* In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001).

[14] Rick Maybury, *How do I find and delete browser cookies?,* THE TELEGRAPH, Jul. 17, 2011, *available at* http://www.telegraph.co.uk/technology/advice/8641184/How-do-I-find-and-delete-browser-cookies.html. *See* Michael King, *How to Delete Cookies*, PCWORLD (Nov. 2, 2011), http://www.pcworld.com/article/242939/how_to_delete_cookies.html.

[15] Jonathan Mayer, *Tracking the Trackers: Microsoft Advertising*, THE CTR. FOR INTERNET AND SOC'Y AT STANFORD L. SCH. (Aug. 18, 2011), http://cyberlaw.stanford.edu/node/6715. *See* Jennifer Valentino-DeVries, *'Supercookie' Code Seen on Hundreds of Sites*, Wall St. J. (Aug. 22, 2011), http://blogs.wsj.com/digits/2011/08/22/supercookie-code-seen-on-hundreds-of-sites/.

[16] *See* LaCourt v. Specific Media, Inc., No. SACV 10–1256–GW(JCGx), 2011 WL 2473399 (C.D. Cal. Apr. 28, 2011) (court dismissed a CFAA claim by individuals who alleged an advertising network installed Flash cookies on users' computers without consent; plaintiff's inability to delete or control cookies may constitute a de minimis injury, but such injury was insufficient to meet the CFAA $5,000.00 threshold).

[17] *See* In re ScanScout, Inc., FTC File No. 1023185 (Settlement announced Oct. 8, 2011) (online advertiser agreed to settle FTC charges that it deceptively claimed that consumers could opt out of receiving targeted ads by changing their browser settings to block cookies, when in fact, the advertiser used Flash cookies that couldn't be blocked by browser settings).

browsing history information associated with that computer and update the cookie.[18] A profile forms over the course of many website visits. Digital profiles become "contextual" maps, drawing on immediate web surfing activities or upon more complex behavioral relationships as software analyzes web surfing data and creates a demographic profile, predicting an age range, likes/dislikes, current interests, level of income and education. Subsequently, when a computer user visits a web page on which the ad network provides advertisements, the network uses a behavioral profile to select tailored advertisements to serve on that computer.[19] Profiles are sold daily to advertisers in online exchanges which nearly instantaneously (while a website is loading) deliver targeted ads to web users.[20]

B. *Legal Landscape*

There are several players in the debate over behavioral advertising and data tracking: (1) privacy watchdog groups advocating for tighter regulation; (2) private litigants who have brought suits over alleged violations of federal electronic privacy laws; (3) Congress and the FTC, which are prompting the industry into implementing tighter self-regulation; and (4) the advertising industry, which has released new self-regulatory principles and technical methods to provide notice and transparency to website users regarding online advertising practices.[21]

Most notably, in December 2010, the FTC stated that the industry's efforts to address privacy through self-regulation have been "too slow" and it continued with its initiative to encourage the industry to offer consumers greater transparency and control with respect to online information gathering. Accordingly, the FTC staff released a report announcing a proposed framework that would apply broadly to online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device.[22] Moreover, the same year, the U.S. Department of Commerce issued its own green paper on data privacy, echoing many of the FTC principles and concerns, and affirming the importance of transparent privacy practices.[23]

In addition, Congress has waded into the debate. There have been a host of bills in both chambers of Congress addressing privacy, online advertising and data tracking.[24] In the Senate, for

---

[18] *Fact and Fiction: The Truth About Browser Cookies*, LIFEHACKER (Feb. 21, 2010), http://lifehacker.com/5461114/fact-and-fiction-the-truth-about-browser-cookies. *See* Alexis Madrigal, *I'm Being Followed: How Google—and 104 Other Companies—Track Me on the Web*, THE ATLANTIC, Mar. 1, 2012, *available at* http://www.nationaljournal.com/tech/i-m-being-followed-how-google-and-104-other-companies-track-me-on-the-web-20120301.

[19] *Id. See also Privacy and Data Security: Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 112th Cong. 3 (2011).

[20] Magrigal, *supra* note 18.

[21] Iab. *Self-Regulatory Program for Online Behavioral Advertising Factsheet, available at* http://www.iab.net/media/file/OBA_OneSheet_Final.pdf.

[22] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS vi, vii (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[23] *See* THE U.S. DEP'T OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (Dec. 2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

[24] *See* Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011).

example, there were at least two bills introduced, most notably, a bill co-sponsored by John Kerry and John McCain (S. 799), the Commercial Privacy Bill of Rights Act of 2011. This would have, among other things, instituted certain security requirements upon data collectors, given individuals the right to opt-out of any information collection that is unauthorized by the Act and provide affirmative opt-in consent for the collection of sensitive information.[25] Both senators have also called upon the FTC to finalize its 2010 preliminary report on online privacy so that the legislation can move forward.[26]

In step with the FTC's policy reports, industry associations have outlined their own set of principles embracing transparency and accountability in an attempt to avoid increased scrutiny and restrictive privacy legislation. The industry has encouraged the use of an 'Advertising Option Icon' that users can click on to obtain basic information on the organization that served the ad, the location of its advertising policy and methods on how to opt-out of such targeted advertisements in the future.[27] Consistent with the accountability provisions in its self-regulatory principles, the Council of Better Business Bureaus recently announced that it had completed compliance cases under the industry's Self-Regulatory Principles for Online Behavioral Advertising against six companies, principally remedying inaccessible or quick-expiring consumer opt-out mechanisms.[28]

In addition, at the end of 2011, the Digital Advertising Alliance, which represents the leading marketing associations, released its "Self-Regulatory Principles for Multi-Site Data" that established industry standards governing the use of so-called "multi-site data," which is web browsing information collected from a computer or other device over an extended time period and across non-affiliated websites. The principles exempt certain practices, including the collection of data for system management, market research or product development, or where the data has or will go through a "de-identification process," which is defined as when an entity "has taken reasonable steps to ensure that the data cannot reasonably be re-associated or connected to an individual or connected to or be associated with a particular computer or device."[29]

C. *'Do Not Track'*

The FTC, in its 2010 staff report, enunciated a privacy framework, including explicit support for a so-called "Do Not Track" option to allow users to limit the collection and use of data regarding their online searching and browsing activities, such as through the placement of a persistent setting

---

[25] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 202 (2011).

[26] The FTC issued its final report on protection of privacy in March 2012. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS (Mar. 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf. *See also* Adam M. Veness, *FTC Issues Long-Awaited Privacy Report*, NAT'L L. REV. Mar. 26, 2012. *See also* John Kerry, *John Kerry: We Need A Commercial Privacy Bill of Rights*, THINK PROGRESS (Mar. 21, 2012), http://thinkprogress.org/justice/2012/03/21/449508/john-kerry-commercial-privacy-bill-of-rights/?mobile=nc.

[27] Iab, *supra* note 21.

[28] Press Release, Better Bus. Bureau, Accountability Program Achieves Voluntary Compliance with Online Behavioral Advert. Self-Regulation (Nov. 8, 2011).

[29] Digital Advert. Alliance, *Self-Regulatory Principles for Multi-Site Data*, 8 (Nov. 2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

on the consumer's browser signaling the consumer's privacy choices.[30] The FTC staff suggested that such a mechanism should be different from the Do Not Call telemarketing program in that it should not require a "registry" of unique identifiers.[31] In its view, the most practical method would likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signaling the consumer's choices about being tracked and receiving targeted ads.[32]

Both Internet Explorer[33] and Firefox have added Do Not Track capabilities to their most recent browsers, though a spokesman for Mozilla's Firefox web browser stated that about 5% of desktop users have turned on the Do Not Track tool (as compared with 17% of mobile users).[34] For users of the browser tool, it is up to the visited websites to honor users' Do Not Track requests and ultimately, it may be difficult for a user to ascertain which websites and ad networks are respecting their choices. In response to this inherent problem, the World Wide Web Consortium, an industry group, released a draft of Do Not Track standards that define the methods for users to indicate their preferences, techniques for websites to inform users whether they honor Do Not Track preferences, and a mechanism for permitting the user to grant site-specific exemptions to their Do Not Track preference.[35]

D. *Geolocation*

The latest generation of smartphones used by consumers lend themselves to numerous other uses beyond basic communication, including mapping and GPS functionalities and a myriad of downloadable personal or business applications—or "apps." Because consumers carry their mobile devices with them at all times, marketers see great potential in providing consumers with real-time, location-based advertising.[36] There are two principal ways location-based advertising works. Geolocation social networks, such as Foursquare, permit users to share their location with friends by "checking-in" to an establishment or venue, which often gives rewards to frequent visitors.[37] In addition to business listings and map locations served on request and ranked by proximity to the user,

---

[30] FED. TRADE COMM'N, *supra* note 22.

[31] *Id.* at 67.

[32] *Id.* at 66.

[33] Nick Wingfield & Julia Angwin, *Microsoft Adds Do-Not-Track Tool to Browser*, WALL ST. J. (Mar. 14, 2011), *available at* http://online.wsj.com/article/SB10001424052748703363904576200981919667762.html. *See* Michael Muchmore, *The State of 'Do Not Track' in Current Browsers*, PCWORLD (Mar. 27, 2012), http://www.pcmag.com/article2/0,2817,2402168,00.asp. *See also* MOZILLA FIREFOX. *Do Not Track,* http://dnt.mozilla.org/.

[34] Alex Fowler, *Mozilla Publishes Developer Guide on DNT; Releases DNT Adoption Numbers*, MOZILLA PRIVACY BLOG (Sept. 8, 2011), http://blog.mozilla.com/privacy/2011/09/08/mozilla-publishes-developer-guide-on-dnt-releases-dnt-adoption-numbers/.

[35] *See* Roy T. Fielding & David Singer, *Tracking Preference Expression (DNT), Working Draft*, WORLD WIDE WEB CONSORTIUM, (Mar. 13, 2012), http://www.w3.org/TR/tracking-dnt/. *See also* Roy T. Fielding, *Tracking Preference Expression (DNT), Working Draft*, WORLD WIDE WEB CONSORTIUM, (Nov. 14, 2011), http://www.w3.org/TR/2011/WD-tracking-dnt-20111114/.

[36] *See* Adrianne Jeffries, *For Advertisers, Location-Based Services "Blew Up Overnight,"* READWRITEWEB (Sept. 8, 2010), http://www.readwriteweb.com/archives/for_advertisers_location-based_services_blew_up_ov.php.

[37] *See* FOURSQUARE, https://foursquare.com/about/ (last visited Apr. 1, 2012). *See also* Corina Mackay, *The Future of Geolocation: What is Coming?*, SOCIAL MEDIA EXAMINER (Apr. 21, 2011), http://www.socialmediaexaminer.com/the-future-of-geolocation-what-is-coming/.

providers are also rolling out location-based mobile advertising platforms that would serve ads to users' mobile phone based on their movements.[38]

Given the personal nature of geolocation, it is not surprising that disputes have arisen over its alleged misuse. For example, in *In re iPhone Application Litigation*, users claimed that Apple violated their privacy rights by unlawfully allowing third-party apps that run on the iPhone and iPad to collect and make use of, for commercial purposes, personal consumer information (including address book, cell phone numbers, geolocation, photographs, SIM information) without user consent.[39] Plaintiffs claimed that such data could be merged to effectively "deanonymize" consumers.[40] The court dismissed the action for lack of standing, with leave to amend.[41] The court found that plaintiffs failed to allege a tangible injury, particularly since the complaint failed to particularize which apps tracked their data, the resulting harm and Apple's culpable conduct.[42,43]

In addition, Apple argued that its terms of service barred claims stemming from third-party apps (e.g., "The Application Provider of each Third-Party Product is solely responsible for that Third-Party Product").[44] Apple also argued that claims based on the design of the iPhone operating system were barred by the iOS Software License Agreements.[45] The court declined to rule that the licenses were an absolute bar, but ordered plaintiffs to explain in an amended complaint why Apple shouldn't be immunized from suit based upon its terms of service.[46] The court also found the plaintiffs' Computer Fraud and Abuse Act (CFAA) claim deficient, because, among other things, negligent software design cannot form a CFAA computer fraud claim.[47]

In response to privacy concerns over geolocation, the mobile phone industry and Congress have advanced potential solutions. There were at least two bills introduced into Congress concerning geolocation privacy.[48] The Senate bill would require any company that obtaining a customer's

---

[38] *See* Erin Griffith, *Is Location-Based Mobile Advertising Real? Answer: yes, according to LocalResponse*, Adweek (Oct. 13, 2011), *available at* http://www.adweek.com/news/technology/location-based-mobile-advertising-real-135758. *See also* Ryan Kim, *Mobile advertisers paying 4x more for location-based impressions*, GIGAOM (Nov. 2, 2011), http://gigaom.com/2011/11/02/mobile-advertisers-paying-4x-more-for-location-based-impressions/.

[39] *In re iPhone Application Litigation*, No. 11–MD–02250–LHK, 2011 WL 4403963 at *2 (N.D. Cal. Sept. 20, 2011).

[40] *Id.*

[41] *Id.* at *7.

[42] *Id.* at *4.

[43] *See also* Low v. LinkedIn, No. 11–CV–01468–LHK, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011) (plaintiffs alleged that a social media site disclosed "personally identifiable browsing histories" to third-party advertising companies via cookies; court dismissed the action, with leave to amend, for lack of Article III standing due to the plaintiffs' failure to allege a particularized harm).

[44] *Id.* at *7.

[45] *Id.*

[46] *Id.* at *8.

[47] *Id.* at *11.

[48] *See* Location Privacy Protection Act of 2011, S.1223, 112th Cong. (2011). *See also* Geolocation and Privacy Surveillance (GPS) Act, S. 1212, 112th Cong. (2011). *See also* Geolocation and Privacy Surveillance (GPS) Act, H.R. 2168, 112th Cong. (2011).

location information from his or her smartphone or other mobile device to (1) get that customer's express consent before collecting the location data; and (2) get that customer's express consent before sharing the location data with third parties.[49]

E. *Regulatory Future*

The growth of geolocation and other new technologies brings the promise of innovative ways to provide consumers with better products and services. However, advances in such technologies stir up privacy concerns. With the release of the online marketing's industry's latest consumer privacy initiatives, it remains to be seen whether such self-regulatory efforts -- the behavioral advertising principles, the 'Advertising Option Icon', the multi-site principles -- will satisfy the FTC and members of Congress currently considering limits on the practice of behavioral advertising and data tracking.

III. LIABILITY ISSUES

As the Internet is being accessed through computers, smartphones, and tablets, consumers, rulemakers, and advertisers alike, are all still discovering the extent to which the broad reach of the Internet can be both helpful and harmful. A number of areas of regulation are fairly unexplored. As a result, certain aspects of Internet use, including use of behavioral/targeted advertising, raise many new and unforeseen legal issues.

Similar to the area of behavioral advertising, another unexplored territory that has become exponentially more serious and complicated due to the growth of the Internet is contributory trademark infringement. Part of the reason for an increase in focus in the legal arena results from the difficulty in tracking the infringers, and the ease of infringement from overseas. This specific area of trademark infringement is tied to the increase in unauthorized sales of goods and sales of knockoff products. As a result of this ability of others to use the Internet for such purposes, trademark owners have shifted their focus to contributory infringers, such as service providers and payment processors, instead of those parties directly infringing on their trademark.[50] The article also explores the state of online trademark infringement and the growing trend of the courts finding service providers, payment processors, or online advertisement network providers liable for contributory trademark infringement. The authors also discuss notice and takedown procedures through various court decisions.

IV. ROLE OF THE INTERNET IN CONTRIBUTORY TRADEMARK INFRINGEMENT

The ubiquity of the Web, on computers, mobile phones, and tablets, offers businesses the opportunity to connect with consumers throughout the world in ways they never could before. Unfortunately, along with the success of legitimate e-commerce, the distribution and sale of counterfeit products through professional-looking websites has also increased dramatically, particularly in the clothing, consumer electronics, pharmaceutical and footwear industries.

---

[49] S.1223, § 3.

[50] *See* Press Release, Dep't of Justice, Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE HSI and FBI Cyber Monday Crackdown (Nov. 28, 2011). *See also* Press Release, U.S. Immigration & Customs Enforcement, Sweetheart, but fake, deals put on ICE "Operation Broken Hearted" protects consumers from counterfeit Valentine's Day goods (Feb. 14, 2011). *See also Louis Vuitton Malletier SA v. Akanoc Solutions, Inc.*, 658 F.3d 936 (9th Cir. 2011).

While estimates of the harm differ greatly among analysts, the sale of counterfeit and knockoff goods has been reported to cost American creators and producers billions of dollars per year.[51] Online infringement harms many facets of the economy: trademark owners suffer lost sales and lost brand value; consumers receive inauthentic products, or, at worst, dangerous goods; and federal and state governments lose tax revenues and incur law enforcement costs.[52] In many cases, consumers are not fully aware of the nature of a transaction, since such virtual stores have legitimate-sounding domain names, often accept payment through major credit card companies, and run online advertisements from trusted providers, all portraying the appearance of legitimacy.

As part of the task of policing their marks, many trademark owners maintain a close watch on counterfeit goods on the Internet and take an aggressive stance against unauthorized uses and sales, including bringing suit against sellers of knockoff goods. However, many so-called rogue web sellers are located abroad and rely solely on digital means to communicate, making it especially difficult to locate and permanently shut them down. As a result, trademark owners have begun to seek recovery from a number of third-party online entities, including Internet service providers, payment processors, and online ad network providers, all of whom may play some role (knowingly or unknowingly) in enabling consumers to access an infringing website, purchase content and products, and view advertisements.

This section will discuss contributory trademark infringement in general and recent actions by trademark owners against online service providers for contributory liability for the sales of counterfeit goods. It will also review the ongoing Congressional debate surrounding online intellectual property infringement.

A. *Contributory Infringement*

Contributory trademark infringement is a judicially created doctrine that derives from the common law of torts. There are two ways in which a party may commit contributory infringement: first, if a provider "intentionally induces another to infringe a trademark," and the second, more commonly pled theory, if a provider "continues to supply its [product or service] to one whom it knows or has reason to know is engaging in trademark infringement."[53] On its face, the *Inwood* test applies to manufacturers and distributors of goods. However, courts have extended the test to service providers that exercise sufficient control over the means of the infringing conduct. Indeed, several circuit courts have determined that a plaintiff must establish that the service provider have "direct control and monitoring of the instrumentality used by a third party to infringe."[54]

B. *Notice and Takedown Principles*

---

[51] Press Release, Patrick Leahy, U.S. Sen. for Vt., Senators Introduce Bipartisan Bill To Combat Online Infringement (Sept. 20, 2010). *See also Targeting Websites Dedicated to Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (Statement of Al Franken, U.S. Sen. for Minn.).

[52] *See* Press Release, Patrick Leahy, U.S. Sen. for Vt., Senate Judiciary Committee Unanimously Approves Bipartisan Bill To Crack Down On Rogue Websites (May 26, 2011). *See also The Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (Statement of Patrick Leahy, U.S. Sen. for Vt.).

[53] Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 854 (1982).

[54] *See* Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980 (9th Cir. 1999). *See also Perfect 10, Inc. v. Visa Intern. Service Ass'n*, 494 F.3d 788 (9th Cir. 2007). *See also Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).

Ultimately, the contours of contributory trademark liability are fashioned by the courts. The Digital Millennium Copyright Act's (DMCA) safe harbors protect qualifying websites and online service providers from copyright liability, and essentially seek to offer strong incentives for service providers and copyright owners to cooperate and deal with online copyright infringement.[55] While there is no similar statutory counterpart under trademark law, in recent years, trademark holders and online providers have borrowed the principles from the DMCA safe harbors in creating a de facto notice and takedown regime to combat the online sale of counterfeit or unauthorized goods. While not mandated by statute, recent court decisions have underscored the importance for online providers of instituting a program for responding to trademark-related takedown notices.

One of the most notable decisions that affirmed this idea was *Tiffany (NJ) Inc. v. eBay, Inc.*, in which an appeals court upheld the judgment in favor of the defendant on the plaintiff's trademark and dilution claims.[56] In that case, the district court found, after a bench trial, that eBay, an online marketplace, had generalized knowledge that some portion of the Tiffany goods sold on its website might be counterfeit, but that such knowledge was insufficient to impose a duty upon eBay to remedy the problem.[57] As such, the court found that eBay was not liable for contributory trademark infringement.[58]

The court specifically held that eBay was not willfully blind and did not ignore the information it was given about counterfeit sales on its website.[59] Rather, eBay spent millions of dollars to identify and remove counterfeit listings and consistently developed and improved its anti-fraud measures.[60] The court rejected the plaintiff's argument that generalized notice that a percentage of the plaintiff's goods being sold on the defendant's site were counterfeit required the site to preemptively remedy the problem.[61]

C. *Liability for Online Service Providers*

Websites selling counterfeit or knockoff goods can be elusive since they are often located abroad, can quickly reappear under a different domain name following a cease and desist letter or adverse judgment, and have no appreciable assets for a plaintiff to recover.[62] As such, aggrieved trademark holders have begun to allege contributory infringement claims against various online

[55] Digital Millennium Copyright Act, 17 U.S.C. § 512 (1998).

[56] *Tiffany*, *supra* note 54.

[57] *Id.* at 107.

[58] *Id.* at 109.

[59] *Id.* at 110.

[60] *Id.* at 100, 109.

[61] *Id.* at 106. *See also Sellify Inc. v. Amazon.com, Inc.*, No. 09 Civ. 10268(JSR), 2010 WL 4455830 (S.D.N.Y. Nov. 4, 2010) (contributory trademark infringement claims dismissed because there was no evidence that Amazon.com had particularized knowledge of, or direct control over, its affiliate's disparaging, keyword-triggered ads and when Amazon gained knowledge of the ads, it acted promptly to disable the affiliate's account).

[62] Press Release, Dep't of Justice, Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE HSI and FBI Cyber Monday Crackdown (Nov. 28, 2011). *See also* Press Release, U.S. Immigration & Customs Enforcement, Sweetheart, but fake, deals put on ICE "Operation Broken Hearted" protects consumers from counterfeit Valentine's Day goods (Feb. 14, 2011).

providers that materially contribute to an online retailer's ability to make a profit off of counterfeit goods. These parties enable U.S. consumers to access the infringing website, purchase content and products, and view advertisements; without the services provided by these entities, the financial incentive to run an infringing website is greatly diminished. In the past year, at least two notable online trademark disputes went to trial, with juries finding in favor of the trademark owner.

In *Louis Vuitton Malletier SA v. Akanoc Solutions, Inc.*, the Ninth Circuit affirmed a jury verdict of contributory trademark infringement against a web host that ignored multiple takedown notices and knowingly enabled infringing conduct by leasing packages of server space, bandwidth and IP addresses to foreign-based websites that sold the plaintiff's knockoff goods.[63] To prevail, the plaintiff had to establish that the defendant continued to supply its services to one who it knew or had reason to know was engaging in trademark infringement and that the defendant had direct control and monitoring over the "means of infringement."[64] The court rejected the defendant's argument that the servers and internet services provided were not the "means of infringement," rather that the websites themselves were the sole means of infringement.[65] Instead, the appeals court stated that even though they exist in cyberspace, "websites are not ethereal" and would not exist without physical roots in servers and internet services and that defendants had direct control over the "master switch" that kept the websites online.[66]

In another dispute, a golf equipment company brought suit against, among others, the web hosting company that participated in the design and support of the websites selling knockoff golf gear.[67] While the defendant web host denied any knowledge that its clients were selling counterfeit golf clubs, the plaintiff countered that beyond offering hosting services, the defendant provided extra coaching and counseling advice to the site operators on search engine optimization, website development, and locating preferred vendors, and otherwise should have known about the nature of the site given its domain name, <www.copycatclulbs.com> and its slogan as the "one stop shop for the best COPIED and ORIGINAL golf equipment on the internet."[68] At trial, a jury found the web host liable for willful secondary trademark infringement and awarded the plaintiff over $770,000 in damages.[69]

Another dispute involving trademark holders was resolved after the threat that a contributory infringement claim might proceed to trial. In *Gucci America, Inc. v. Frontline Processing Corp.*, the court found that a national retailer could proceed with contributory infringement claims against various credit card processors based upon sufficient allegations that the providers exerted sufficient control over the infringing transactions and knowingly provided its services to an internet merchant

---

[63] Louis Vuitton Malletier SA v. Akanoc Solutions, Inc., 658 F.3d 936, 940, 941 (9th Cir. 2011).

[64] *Id.* at 942.

[65] *Id.*

[66] *Id.* at 942-943.

[67] Roger Cleveland Golf Co., Inc. v. Prince, No. 09-02119 (D. S.C. filed Mar. 14, 2011).

[68] Roger Cleveland Golf Co., Inc. v. Price, No. 2:09-CV-2119-MBS, 2010 WL 5019260, at *1, *3 (D. S.C. Dec. 3, 2010).

[69] Roger Cleveland, *supra* note 67.

that sold "replica" products.[70] The court denied the defendants' motion to dismiss, concluding that the defendants facilitated the replica website's ability to efficiently transact sales for counterfeit products by enabling customers to use personal credit cards to pay for purchases.[71]

The court found that the plaintiff made substantial allegations that the defendants knew that the replica site traded in counterfeit products, or were willfully blind to that fact, including: one defendant charged a higher transaction fee for processing credit cards for high risk replica goods merchants; and another helped the counterfeit goods website set up a system to avoid chargebacks, requiring customers to check a box that said "I understand these are replicas" and otherwise assisted in refund requests from customers that necessitated an investigation of products sold.[72]

Notably, the *Gucci* court distinguished the case from *Perfect 10, Inc. v. Visa Int'l Service Ass'n*, where the Ninth Circuit declined to hold a credit card processor liable for contributory trademark and copyright infringement for the unauthorized reproduction and display of Perfect 10's images by certain websites and users.[73] The court pointed out that in the *Perfect 10* dispute, the plaintiff failed to allege that the credit card service provider had the "power to remove infringing material" because the infringement occurred on the third-party websites and a credit card transaction was not needed for the websites to continue posting infringing photographs.[74] In the *Gucci* case, however, the court stated that the plaintiff's allegations were concerned primarily with the sale of tangible counterfeit goods to customers, which allegedly could not be accomplished without the defendants' ability to process the credit card-based purchases.[75]

Beyond payment processors and website design and management providers, at least one court has considered the secondary liability (in the copyright context) of an online advertising network company that placed third-party advertisements on an allegedly infringing website and shared the proceeds with the website owner. In *Elsevier Ltd. v. Chitika, Inc.*, the court found that an online advertising provider that was not familiar with the content of an allegedly infringing free download site and had not received any notice of infringing activity from the plaintiff was not liable for contributory copyright infringement.[76] The court also noted, in dicta, that the defendant did not "materially contribute to the infringement" merely because the shared advertising revenue made it easier for the website owner's infringement to be profitable.[77]

D. *'Rogue Website' Legislation*

Recent court decisions have given trademark holders some ammunition in seeking recovery for infringement against responsible service providers. Regardless, rights holders maintain that they still

---

[70] Gucci America, Inc. v. Frontline Processing Corp., 721 F.Supp.2d 228, 253 (S.D.N.Y. 2010).

[71] *Id.* at 252-253.

[72] *Id.* at 249, 252.

[73] Perfect 10, Inc. v. Visa Inte'l Service Ass'n, 494 F.3d 788, 804-805 (9th Cir. 2007).

[74] *Id.* at 807.

[75] *Gucci America*, *supra* note 70, at 252-253.

[76] Elsevier Ltd. v. Chitika, Inc., No. 11–10026–RGS, 2011 WL 6008975 at *4-5, (D. Mass. Dec. 2, 2011).

[77] *Id.* at *5-6.

possess a limited number of effective remedies to fight online purveyors of infringing goods, particularly legal tools that would hamper websites located abroad from continuing to sell infringing goods on the Internet.[78,79]

V. CONCLUSION

As this piece illustrates, the Internet is a vast, ever-changing, and expanding technology that continues to create new and unforeseen legal issues for regulators, advertisers, and consumers alike.

[78] Press Release, Patrick Leahy, U.S. Sen. for Vt., Leahy: Senate Should Focus On Stopping Online Theft That Undercuts Economic Recovery (Jan. 23, 2012).

[79] Congress has tried to seek a legislative solution that would give the Department of Justice and content owners an expedited process for cracking down on U.S.-directed foreign rogue websites that traffic in pirated or counterfeit goods or digital entertainment.