CONTENTS

Choose Your Words Wisely: Affirmative Representations as a Limit on § 230 Immunity
Jeffrey R. Doty 259

United States v. Berger: The Rejection of Civil Loss Causation Principles in Connection with Criminal Securities Fraud
James A. Jones II 273

Gimme a Brekka!: Deciphering “Authorization” Under the CFAA and How Employers Can Protect Their Data
Amber L. Leaders 285

A Survey of the DMCA’s Copyright Management Information Protections: The DMCA’s CMI Landscape after All Headline News and McClatchey
Susuk Lim 297
Since its enactment in 1996, § 230 of the Communications Decency Act has shielded Web site operators from liability arising out of third-party content. The statute preempts any claim that would treat the defendant as a “publisher” or “speaker” of that content, but recent cases suggest that a defendant’s own statements may constitute an independent source of liability beyond the scope of § 230. In Mazur v. eBay, a federal district court held that § 230 does not bar claims of fraudulent misrepresentation when a defendant has described a third party’s auctioning procedures as “safe.” More recently, the Ninth Circuit in Barnes v. Yahoo! allowed a promissory estoppel claim to proceed against a defendant that failed to remove defamatory material from its Web site after assuring the plaintiff it would do so. A third case, Goddard v. Google, suggests that the Barnes decision could support claims by third-party beneficiaries as well. This Article analyzes these recent developments, discusses their potential impact on representations in marketing and terms of use, and assesses the willingness of courts to consider more expansive fraud- and contract-based limitations on § 230 immunity.
TABLE OF CONTENTS

Introduction ................................................................................................. 260
I. A Three-Part Test for Immunity ............................................................. 261
II. Early Attempts at Establishing an Alternative Basis for Liability ............ 262
III. Fraudulent Misrepresentation in Mazur v. eBay ................................. 263
V. Strategies for Maintaining Immunity ...................................................... 268
VI. A New Direction for CDA Jurisprudence? .......................................... 269
Conclusion .................................................................................................. 270
Practice Pointers ........................................................................................ 270

INTRODUCTION

Section 230 of the Communications Decency Act (CDA)\(^1\) shields Web site operators from liability by barring causes of action that would treat them as the “publisher” or “speaker” of third-party content.\(^2\) Courts have been willing to apply its provisions to virtually any kind of dispute involving third-party content.

However, a recent line of cases suggests that a Web site operator’s affirmative representations regarding its third-party content could create an alternative basis for liability to which § 230 does not apply. In Mazur v. eBay,\(^3\) a federal district court held that § 230 did not bar a claim of fraudulent misrepresentation, and in Barnes v. Yahoo!,\(^4\) the Ninth Circuit allowed a promissory estoppel claim to proceed on the grounds that it did not treat the defendant as a “publisher.” A more recent case, Goddard v. Google,\(^5\) suggests that the Barnes holding could support claims by third-party beneficiaries as well. These cases reveal that affirmative representations can give


\(^4\) Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009).

rise to liability if they amount to fraudulent misrepresentation or constitute an enforceable promise, creating potential pitfalls for online businesses with respect to marketing, customer service, and even user agreements.

This Article first provides an overview of § 230 and the early attempts by plaintiffs to establish liability without treating the defendant as a publisher. Next, the Article analyzes the recent cases that have begun to recognize a limit on § 230 immunity based on a defendant’s own representations. The Article concludes by discussing how these decisions are shaping CDA jurisprudence and the implications for Web site operators.

I. A THREE-PART TEST FOR IMMUNITY

Section 230 was designed, in part, to allow Web site operators to voluntarily monitor their sites for offensive or obscene material without exposing themselves to liability for third-party content. The statute declares that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”

To determine whether a defendant is entitled to immunity, courts engage in a three-part analysis. First, the defendant must be a “provider or user of an interactive computer service.” This effectively encompasses all Web sites. Next, because the scope of § 230 extends only to third-party content, the defendant will not receive immunity if it is “responsible … for the creation or development” of the offending content. Finally, the cause of action must treat the defendant as the “publisher” or “speaker” of the

---

8. See, e.g., Universal Comme’n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 418–22 (1st Cir. 2007).
10. The Internet itself qualifies as an “interactive computer service,” and therefore, a defendant need only be a “user” of the Internet to satisfy the first prong of the test. Because every Web site operator is necessarily an Internet user, this requirement is rarely the subject of litigation. See Batzel v. Smith, 333 F.3d 1018, 1030–31 (9th Cir. 2003).
content.\textsuperscript{12} Claims that would hold the defendant liable in some other capacity are unaffected by § 230.\textsuperscript{13} It is this distinction that makes affirmative representations potentially problematic.

II. EARLY ATTEMPTS AT ESTABLISHING AN ALTERNATIVE BASIS FOR LIABILITY

To avoid treating the defendant as a publisher, plaintiffs have long sought to base their claims on actions by the defendant that go beyond a publisher’s “traditional editorial functions,”\textsuperscript{14} thereby providing an independent basis for liability. For instance, in \textit{Blumenthal v. Drudge}\textsuperscript{15} the plaintiff argued that AOL could be held liable for the defamatory material of co-defendant Matt Drudge because AOL had “affirmatively promoted Drudge as a new source of unverified instant gossip.”\textsuperscript{16} The court nevertheless concluded that the language of § 230 clearly protected the decision to advertise third-party content.\textsuperscript{17} In \textit{Schneider v. Amazon.com, Inc.},\textsuperscript{18} a defendant had promised to remove certain offensive postings within two business days but failed to do so.\textsuperscript{19} Although the plaintiff argued that this promise constituted an independently enforceable obligation, the court determined that it fell within the scope of § 230 because the “purported breach—failure to remove the posting—[was] an exercise of editorial discretion.”\textsuperscript{20} Courts have also rejected arguments based on a defendant’s failure to enforce standards of conduct set out in its membership agreement.\textsuperscript{21} As these early cases illustrate, plaintiffs

\textsuperscript{13} See, e.g., Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1107 (9th Cir. 2009) (denying immunity where defendant breached an independent contractual duty).
\textsuperscript{14} “Traditional editorial functions” include “deciding whether to publish, withdraw, postpone or alter content.” See Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).
\textsuperscript{16} Id. at 51.
\textsuperscript{17} Id. at 52–53.
\textsuperscript{19} Id. at 38–39.
\textsuperscript{20} Id. at 42.
have historically been unsuccessful at suing defendants for third-party material without also treating them as publishers.

III. FRAUDULENT MISREPRESENTATION IN MAZUR V. EBAY

The ruling in Mazur v. eBay, however, put Web site operators on notice that their own statements regarding third-party content could carry significant consequences. In Mazur, the defendant offered a service called Live Auctions, which allowed users to participate in formal auctions via the Internet as if they were physically there. Third-party auction houses conducted the auctions; eBay merely provided the service that allowed people to place bids at these auctions over the Internet. On its Web site, eBay claimed that the service was “very safe,” that the live auctions involved “floor bidders,” and that the auctions were conducted by “reputable international auction houses” that were “carefully screened.” Nevertheless, the plaintiff alleged that shill bidders at the auction house caused her to overpay. She sued eBay, claiming that its statements regarding the live auctions amounted to fraudulent misrepresentation.

The court analyzed each of eBay’s assertions independently. It determined that eBay was entitled to immunity for its representation that the auction houses were “reputable” and “carefully screened.” The court explained that “screening” auction houses is analogous to deciding what to publish, and is therefore a traditional editorial function shielded by § 230. Furthermore, the words “carefully” and “reputable” indicate opinions, which are not actionable.

However, eBay’s assertions that the live auctions were “safe” and

25 “Shill bidding” is the practice of entering fake bids in order to drive up the price of an auction item.
27 Id.
28 Id.
involved “floor bidders” at “international” auction houses were held to be actionable as affirmative representations. 29 According to the opinion, these statements went beyond traditional editorial discretion because they created “an expectation regarding the procedures and manner in which the auction is conducted.” 30 The court indicated that if eBay had made assurances of accuracy, it would have received immunity, as verifying accuracy constitutes a traditional editorial function. 31 Assurances of safety, however, would fall outside the scope of § 230. 32

The court also determined that eBay’s disclaimers were ineffective for two reasons. First, they failed to negate either the assurance of safety or the implicit suggestion that eBay had investigated the auction houses. 33 Although eBay stated in its User Agreement that it had no control over the safety of the auctions and could not guarantee that the auction houses complied with applicable laws, “nothing [in the User Agreement] specifically state[d] that eBay [did] not guarantee that bidding in Live Auctions [was] safe.” 34 Second, eBay failed to demonstrate that the initial safety assurances were attributable to another source, such as user feedback. 35 As a result, users could not independently assess the veracity of the claim and were left to depend on eBay’s representations. Having made the statements on its own behalf, eBay could no longer rely on general disclaimers applicable to third-party conduct.

IV. CONTRACTUAL LIABILITY IN BARNES V. YAHOO! AND GODDARD V. GOOGLE

A defendant’s liability is not limited to fraud, however. A recent Ninth Circuit case demonstrates that affirmative representations can furnish the basis for liability under contract principles as well.

29 Id. at *10.
30 Id. at *12.
31 See id. See also Milo v. Martin, 311 S.W.3d 210 (Tex. App. 2010) (finding defendant not liable for the defamatory posts of users, despite assurances of accuracy found elsewhere on its Web site).
32 See Mazur, 2008 WL 618988, at *12.
33 Id. at *10.
34 Id. at *11.
35 Id. at *10.
In *Barnes v. Yahoo!*, the plaintiff discovered that her ex-boyfriend had created fake profiles under her name on a Yahoo! Web site. Over the next two months, Barnes made four requests to have the profiles taken down, but Yahoo! never responded to any of them. Finally, as local news prepared to broadcast a report on the incident, a representative from Yahoo! contacted Barnes and told her that she would “personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it.” Despite this assurance however, the profiles remained on the Web site until Barnes filed suit two months later, alleging promissory estoppel and negligent undertaking.

The court held that § 230 did not preempt a promissory estoppel claim arising out of the defendant’s promise to remove third-party content from its Web site. According to the opinion, such a claim would not seek to treat the defendant as a “publisher.” Instead, it was the defendant’s promise, and not its status as a publisher, that gave rise to liability. The court did, however, hold that § 230 barred the plaintiff’s negligent undertaking claim, explaining that if the action the defendant undertook to do was “something [that] publishers do,” then the cause of action would seek to hold the defendant liable as a publisher. In this case, the “duty” allegedly violated stemmed from Yahoo!’s conduct as a publisher—“the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive profiles.”

The two claims differed in one important respect. “Undertake” is synonymous with the performance of the action; “[t]o undertake a thing ... is to do it.” In contrast, one can promise to do something without actually doing it. Consequently, a defendant cannot be held

---

36 Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009).
37 Id. at 1098.
38 Id.
39 Id. at 1098–99.
40 Id. at 1099.
41 Id. at 1109.
42 Id. at 1107.
43 Id.
44 Id. at 1107.
45 Id.
46 Id. at 1103.
liable for undertaking an editorial action, but it can be liable for breaking a promise, even if that promise was to undertake an editorial action. The promise itself gives rise to a duty that is distinct from the conduct at hand.

A federal district court in Goddard v. Google has since concluded that the rule in Barnes would also permit claims by third-party beneficiaries. “Theoretically, intended third-party beneficiaries—whose rights under a contract are different from those of the contracting parties but still are legally cognizable—could invoke the distinction drawn in Barnes between liability for acts that are coextensive with publishing or speaking and liability for breach of an independent contractual duty.” The plaintiff in Goddard was an Internet user who incurred fees after downloading purportedly “free” ringtones from a Web site that appeared as a “sponsored result” on the defendant’s search engine. The terms of Google’s advertising contracts required advertisers to disclose information about any fees they might charge. Because the advertisement that appeared on Google’s Web site lacked such information, the complaint alleged that Google had breached the terms of its advertising contracts. The plaintiff claimed to be a third-party beneficiary of those contracts.

Though the court acknowledged the possibility of suits by third-party beneficiaries, it nonetheless dismissed the plaintiff’s claim, citing two flaws. First, it was the advertisers, not Google, who promised to disclose information about fees and who subsequently broke that promise. The contracts did not contain any promise by Google to enforce their terms or to remove noncompliant

---

47 See id. ("Contract liability here would come not from Yahoo’s publishing conduct, but from Yahoo’s manifest intention to be legally obligated to do something, which happens to be removal of material from publication.")


49 Id. at 1200.

50 Id.

51 Id. at 1194, 1197.

52 Id. at 1199.

53 Id.

54 Id.

55 Id. at 1200–01.

56 Id. at 1201.
advertisements. Second, even if Google had promised to police its Web site for noncompliant advertisements, there was no indication that the promises (the advertising companies) had intended for the plaintiff to benefit from such a promise. The plaintiff therefore did not qualify as a third-party beneficiary.

The contractual theory of liability that emerges from *Barnes* and *Goddard* is subject to two important limitations that distinguish it from the approach seen in *Mazur*. The *Barnes* court stressed that a promise must be clear and specific if it is to support a promissory estoppel claim: “[A] court cannot simply infer a promise from an attempt to de-publish of the sort that might support tort liability” under a theory of promissory estoppel. The *Goddard* court explained that “general content policies” do not constitute a promise by the Web site to take any specific action with regard to third-party content. A general claim of safety, such as the one in *Mazur*, would likely fail to meet this specificity requirement.

The other critical distinction between the two theories is that, under *Barnes*, a potential defendant can avoid liability by simply disclaiming any intent to be legally bound. In contrast, the *Mazur* opinion would seem to limit the availability of disclaimers to situations where the Web site operator has either explicitly disavowed its own statements or clearly indicated that those statements are attributable to a source other than itself.

---

57 Id. ("Neither agreement contains any promise by Google to enforce its terms of use or otherwise to remove noncompliant advertisements.")

58 Id. The court stated that Goddard might well be able to sue the advertisers for breaching their promise to abide by the Advertising Terms if she could demonstrate that Google had intended for her to be a beneficiary of that agreement.

59 Id.

60 *Barnes v. Yahoo!*, 570 F.3d 1096, 1108 (9th Cir. 2009).

61 *Goddard*, 640 F. Supp. 2d at 1201. It should be noted that although the *Barnes* court did not address whether the actual statement by the Yahoo representative would suffice for purposes of promissory estoppel, the *Goddard* opinion suggests that it would. “[T]he claim in *Barnes* … rested on a promise that scarcely could have been clearer or more direct.” Id.

62 See *Barnes*, 570 F.3d at 1108.
V. STRATEGIES FOR MAINTAINING IMMUNITY

As a result of these developments, Web site operators run the risk of sacrificing § 230 immunity when they issue statements regarding their third-party material. However, a Web site operator may be able to minimize its exposure by taking certain measures.

When promoting a product or service, a Web site operator must have a clear understanding of the message being conveyed. If an affirmative representation tends to suggest that a particular harm will not occur in connection with that product or service, the Web site operator could be viewed as having voluntarily assumed responsibility for its third-party content.63 Similarly, if a Web site operator imposes restrictions in its user agreement on the type of material that third parties can post, it might inadvertently assume a duty to enforce those standards by blocking or removing offensive material. Any statements to this effect should include language alerting users to the possibility that nonconforming content may appear on the site.64

The form of the representation warrants particular attention. Anything phrased as a promise or assurance has the potential to bind the Web site operator, so companies should instruct their employees to avoid making such statements to outside parties. Because representations of fact are actionable, Web sites should consider phrasing that would tend to indicate an opinion. Along the same lines, it may be helpful to insert language into a representation that relates back to an editorial function. The Mazur court indicated that a plaintiff could not sue a Web site for commenting on its own publishing activities, as doing so would treat the defendant as a publisher.65

To avoid falling victim to the contractual theories of liability

developed in the *Barnes* and *Goddard* cases, one should always disclaim any intent to be legally bound. This is especially important when the Web site is providing assistance or otherwise responding to user requests. Furthermore, if the Web site is contracting with another party, such as an advertiser, the contract should specify that no one other than the contracting parties is intended to be a beneficiary of the agreement.

As the *Mazur* case illustrates, however, Web site operators will not always be able to protect themselves through the use of disclaimers. The court made it clear that if it is to be effective at all, a disclaimer must *specifically negate* the affirmative representation,\(^\text{66}\) although given the court’s manifest hostility toward their use,\(^\text{67}\) it is doubtful that disclaimers would ever be effective under the *Mazur* standard.

Whenever possible, a Web site will want to attribute a representation to some source other than itself. For example, the *Mazur* court indicated that eBay would have been entitled to immunity had its assertion of safety been made on the basis of user feedback, rather than its own independent assessment.\(^\text{68}\) Web sites can avoid responsibility by indicating that the representation originated elsewhere. If, on the other hand, a particular statement represents an assertion by the Web site itself, the threat of litigation can be minimized by disclosing the basis for these assertions or the criteria used to reach a particular conclusion. This allows users to evaluate the claims for themselves.

### VI. A NEW DIRECTION FOR CDA JURISPRUDENCE?

Given the highly fact-dependent nature of their holdings, it is unlikely that these recent decisions will appreciably alter the balance

---

\(^{66}\) See *id.* at *10–11.

\(^{67}\) The court determined that eBay’s disclaimers were ineffective despite language such as “We have no control over the quality, safety, or legality of the items advertised” and “You will not hold eBay responsible for other users’ actions or inactions, including things they post.” *See id.* at *10, n.9; *12. Citing the fact that eBay “buried” the disclaimer in a User Agreement and possessed “superior bargaining power,” the court stated that it would deny eBay’s motion to dismiss if the affirmative representation and the disclaimer were contradictory. *Id.* at *13.

\(^{68}\) *Id.* at *10.
of power in § 230 disputes. However, while these cases—Mazur, Barnes, and Goddard—represent developments at the margins, they may nevertheless reflect a conscious effort by the judiciary to prevent an already generous grant of immunity from expanding further. When it came to their publishing activities, Web site operators once faced virtually no threat of liability, but a more nuanced application of § 230 creates new avenues for plaintiffs to explore. The idea that immunity can be lost by “affirmatively promoting” content, ultimately rejected in Blumenthal, has gained traction in the wake of Mazur. Whereas Schneider had extended immunity to contract claims if the breach resulted from an exercise of editorial discretion, Barnes now imposes liability under virtually identical facts. Even a contract between a Web site and an advertiser may create enforceable rights in other parties under the reasoning of Goddard. Plaintiffs are sure to test the limits of these emerging theories in future cases.

CONCLUSION

Although § 230 of the CDA preempts any cause of action that would treat the defendant as a “publisher” or “speaker” of third-party content, recent cases demonstrate that suits premised on a Web site operator’s own statements do not necessarily fall within this category. As a result of Mazur v. eBay, Barnes v. Yahoo!, and Goddard v. Google, affirmative representations regarding third-party content may now serve as an independent source of liability if they amount to fraudulent misrepresentation or constitute an enforceable promise. These developments will affect how Web sites can market third-party content, interact with users, and form agreements with other parties.

PRACTICE POINTERS

- Although § 230 provides protection against liability arising out of third-party content, Web site operators remain fully responsible for the accuracy of their statements regarding that content.
- Section 230 provides no defense to binding contracts created under the theory of promissory estoppel, even when the statement giving rise to the obligation revolves around third-party content.
- Disclaimers may be sufficient to protect a Web site operator
against promissory estoppel claims, but they are unlikely to protect against claims of fraudulent misrepresentation.

- Web site operators can reduce the threat of litigation by either explaining the basis for their affirmative representations or attributing them to another source.
UNITED STATES v. BERGER: THE REJECTION OF CIVIL LOSS CAUSATION PRINCIPLES IN CONNECTION WITH CRIMINAL SECURITIES FRAUD

James A. Jones II*
© James A. Jones II

Cite as: 6 Wash J.L. Tech. & Arts 273 (2011)
http://hdl.handle.net/1773.1/1035

ABSTRACT

In United States v. Berger, a Ninth Circuit panel declined to apply the civil loss causation principles established by the United States Supreme Court in Dura Pharmaceuticals, Inc. v. Broudo in connection with sentencing in a criminal securities fraud prosecution. The Ninth Circuit declined to follow Second and Fifth Circuit decisions endorsing the application of Dura Pharmaceuticals to criminal sentencing, creating a circuit split. This Article examines this split over how to apply the loss causation principles of Dura Pharmaceuticals in connection with sentencing in criminal securities fraud prosecutions. In addition, this Article discusses the implications of each approach for criminal securities fraud prosecutions, and more specifically, for sentencing.

TABLE OF CONTENTS

Introduction .............................................................................. 274
I. The Supreme Court’s Decision in Dura Pharmaceuticals, Inc. v. Broudo .............................................................. 275

* James A. Jones II, CPA, University of Washington School of Law, Class of 2011; University of Washington Foster School of Business, MPAcc, 2006. Thank you Professor Jane K. Winn of the University of Washington School of Law and student editor Jennifer Heidt White for your valuable feedback. Thank you also Professor Scott A. Schumacher of the University of Washington School of Law for your thoughtful review of this Article.
II. Application of Loss Causation Principles to Criminal Securities Fraud Sentencing ............................................................... 276
   A. Loss Under the U.S. Sentencing Guidelines......................... 277
   B. The Fifth Circuit’s Decision in United States v. Olis..... 279
   C. The Second Circuit’s Decision in United States v. Rutkoske ........................................................................ 280
III. The Ninth Circuit Declines to Apply Loss Causation Principles in Connection with Criminal Securities Fraud Sentencing .............................................................................. 281
IV. Implications of the Ninth Circuit’s Decision in United States v. Berger .............................................................. 283
Conclusion................................................................................ 284

INTRODUCTION

In 2005, the Supreme Court resolved a circuit split by holding in *Dura Pharmaceuticals, Inc. v. Broudo*¹ that a private plaintiff claiming securities fraud must show both that the alleged fraud was disclosed to the market and the disclosure caused a loss to shareholders, that is, that the share price fell after the defendant’s fraud became known. No longer could civil plaintiffs merely allege that the price of a security was inflated on the date of the purchase because of a defendant’s misrepresentation. Although the Supreme Court’s decision applied to loss calculation in civil securities fraud cases, the Second and Fifth Circuits have since suggested that the loss causation principles described in *Dura Pharmaceuticals* also apply in sentencing for criminal securities fraud cases.²

In *United States v. Berger*, the Ninth Circuit diverged from the Second and Fifth Circuits and held that federal judges need not follow the loss causation principles that apply in private securities actions when calculating the amount of loss for U.S. Sentencing Guidelines purposes in criminal securities fraud cases.³ This ruling could have a profound effect on criminal securities fraud prosecutions in the Ninth Circuit, resulting in sentencing enhancements for

---

² *See* United States v. Rutkoske, 506 F.3d 170 (2d Cir. 2007); United States v. Olis, 429 F.3d 540 (5th Cir. 2005).
³ United States v. Berger, 587 F.3d 1038 (9th Cir. 2009).
defendants in criminal securities fraud cases where “fraud-on-the-market” formed the basis of the shareholders’ losses.

This Article explores the Supreme Court’s decision in *Dura Pharmaceuticals* as it applies to loss causation in civil securities fraud cases. This Article then examines the U.S. Sentencing Guidelines and the importance of loss calculation in sentence determination. Next, this Article examines the split among the Second, Fifth, and Ninth Circuits in applying the loss causation principles of *Dura Pharmaceuticals* in connection with sentencing in criminal securities fraud prosecutions. Finally, this Article addresses the implications of each approach on criminal securities fraud prosecutions, and more specifically, on sentencing.

I. THE SUPREME COURT’S DECISION IN DURA PHARMACEUTICALS, INC. V. BROUDO

In *Dura Pharmaceuticals, Inc. v. Broudo*, the Supreme Court addressed whether a plaintiff could satisfy the loss causation requirement simply by establishing that the price of the security on the date of purchase was inflated because of the defendant’s misrepresentation. The plaintiffs were a class of individuals who bought stock in Dura Pharmaceuticals, Inc. (Dura) on the public securities market between April 15, 1997, and February 24, 1998. The plaintiffs alleged that during that period, Dura’s managers and directors allegedly made false statements regarding the company’s profits and prospects for future approval of its products by the Food and Drug Administration (FDA).

On February 24, 1998, Dura announced that its earnings would be lower than expected, and the company’s shares lost almost half their value in trading the next day. Nine months later, Dura announced that the FDA would not approve its new product, resulting in another drop in its share price. The plaintiffs argued that they suffered damages by paying artificially inflated prices for Dura securities in

---

5 *Id.* at 339.
6 *Id.*
7 *Id.* (falling from about $39 per share to about $21).
8 *Id.*
reliance on the integrity of the market.  

The Court recognized that an inflated purchase price in itself does not necessarily equate to or proximately cause the economic loss. At the time of initial purchase, the stock still reflects an economic value of the inflated purchase price. If the purchaser sells the stock at that instant, or at any other time before the truth of the misrepresentation becomes public, the purchaser will not have realized any loss. Even if the purchaser sells the stock at a lower price subsequent to the public release of the relevant truth, the lower price "may reflect, not the earlier misrepresentation, but changed economic circumstances, changed investor expectations, new industry-specific or firm-specific facts, conditions, or other events, which taken separately or together account for some or all of that lower price." From this, the Court reasoned that "the most logic alone permits . . . is that the higher purchase price will sometimes play a role in bringing about a future loss."  

For these reasons, and relying on the common-law roots of securities fraud actions, which have long required that a plaintiff show actual damages, the Court held that an investor must show that the fraud was publicly revealed and that the public disclosure caused the investor’s loss. In other words, an investor may not establish loss causation by alleging that the security price was inflated because of the defendant’s misrepresentation. In effect, the Court rejected the notion that stock over-valuation resulting from so-called “fraud-on-the-market” may form the basis for a plaintiff’s damages award in a private securities action.

II. APPLICATION OF LOSS CAUSATION PRINCIPLES TO CRIMINAL SECURITIES FRAUD SENTENCING

Although the Supreme Court has not applied its Dura

---

9 Id. at 340.
10 Id. at 342.
11 Id. at 342-43.
12 Id.
13 Id. at 343.
14 Id. at 345-47.
15 Id. at 341-43.
Pharmaceuticals loss causation principles to sentencing enhancements in criminal securities fraud cases, two federal circuit courts have applied the principles in such a context. In United States v. Olis, the Fifth Circuit determined that the civil loss causation principles described in Dura Pharmaceuticals should inform criminal securities fraud sentencing. The Second Circuit endorsed the application of Dura Pharmaceuticals’ principles to criminal sentencing in United States v. Rutkoske. However, before discussing Olis and Rutkoske, it is necessary to examine the importance of loss calculation in a criminal setting under the U.S. Sentencing Guidelines.

A. Loss Under the U.S. Sentencing Guidelines

Using a detailed set of rules, tables, and adjustments that look at the entire conduct of a convicted defendant, the U.S. Sentencing Guidelines produce a numerical score, or “offense level,” which then translates into a range of months of imprisonment. Since the Supreme Court’s decision in United States v. Booker, federal district judges are no longer required to impose a sentence within the U.S. Sentencing Guidelines. They nonetheless remain obligated to calculate and consider the applicable sentencing range under the U.S. Sentencing Guidelines. Therefore, the calculation of “loss” under the U.S. Sentencing Guidelines remains a critical issue at sentencing in criminal securities fraud cases.

A defendant’s sentence in a securities case can depend heavily on the calculation of loss under the U.S. Sentencing Guidelines. Section 2B1.1 of the U.S. Sentencing Guidelines governs the sentencing calculation for fraud-based crimes, including criminal securities fraud. This section provides a base offense level for fraud-based

---

17 Id. at 246 (“make the Guidelines system advisory while maintaining a strong connection between the sentence imposed and the offender’s real conduct”).
18 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 (2010). It should be noted that Section 2F1.1 of the U.S. Sentencing Guidelines used to govern the sentencing calculation for fraud-based crimes but was consolidated into Section 2B1.1 along with the guidelines for theft and property destruction, effective November 1, 2001. See U.S. SENTENCING GUIDELINES MANUAL app. C, amend. 617 (2010). Section 2F1.1 was applied at the trial court in both United States v. Berger and United States v. Rutkoske. See United States v. Berger, 587 F.3d 1038, 1044-45 (2d Cir.
crimes, which may be increased depending on various factors, including the amount of loss attributed to the offense. The U.S. Sentencing Guidelines explain that “loss serves as a measure of the seriousness of the offense and the defendant’s relative culpability and is a principal factor in determining the offense level under this guideline.”\(^{19}\) As the amount of loss increases, the offense level calculation increases, and thus the sentence increases.\(^{20}\) These increases range from zero for losses of $5,000 or less, to as many as 30 for losses exceeding $400 million.\(^{21}\) For a defendant charged with criminal securities fraud, the difference between a loss of $0 and a loss exceeding $400 million can mean the difference between probation and more than 19 years in prison.\(^{22}\)

Guidance for determining the meaning of “loss” within the U.S. Sentencing Guidelines is found in Application Note 3 of Section 2B1.1.\(^{23}\) Courts are expected to apply the greater of actual loss or intended loss.\(^{24}\) In determining the actual or intended loss attributable to a defendant’s conduct, the U.S. Sentencing Guidelines require only that courts make a reasonable estimate of the loss, given the available information.\(^{25}\) Due to the deference given to sentencing judges, courts have used a variety of methods to calculate losses under the U.S. Sentencing Guidelines.\(^{26}\)

---

\(^{19}\) U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. background.

\(^{20}\) Id. at § 2B1.1(b)(1).

\(^{21}\) Id.

\(^{22}\) Assuming no other enhancements, a first-time offender involved in a fraudulent scheme resulting in a loss of $5,000 or less faces a sentencing range of zero to six months. See U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(a)(2010); U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(1)(A) (2010); U.S. SENTENCING GUIDELINES MANUAL ch. 5, pt. A (2010). If the loss exceeds $400 million, that same defendant would be subject to a 30-level increase to the base offense level, resulting in a sentencing range of 188-235 months. See U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(1)(P) (2010); U.S. SENTENCING GUIDELINES MANUAL ch. 5, pt. A (2010).

\(^{23}\) U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3 (2010).

\(^{24}\) Id.

\(^{25}\) Id. at § 2B1.1 cmt. n.3(C).

\(^{26}\) See United States v. Holliman, 291 F.3d 498 (8th Cir. 2002) (relying on losses arising from the defendant’s relevant conduct); United States v. Piggie, 303 F.3d 923 (8th Cir. 2002) (relying on intended loss); United States v. Manas, 272
The deference given to sentencing judges has resulted in uncertainties in how loss is calculated. Combined with the great significance given the loss figure by the U.S. Sentencing Guidelines, this deference has become a primary source of concern for defendants and their counsel in criminal securities fraud cases. The following federal circuit court decisions address this concern in applying *Dura Pharmaceuticals* loss causation principles to sentencing enhancements in criminal securities fraud cases.

### B. The Fifth Circuit’s Decision in United States v. Olis

The Fifth Circuit became the first appellate court to extend the *Dura Pharmaceuticals* decision to criminal securities fraud cases in *United States v. Olis*.\(^{27}\) James Olis was sentenced to 292 months in prison for securities fraud, mail and wire fraud, and conspiracy arising from his work as Senior Director of Tax Planning and International (and later, Vice President of Finance) at Dynegy Corporation (Dynegy) on a transaction called “Project Alpha.”\(^{28}\) The offense level was “extraordinarily high” as a result of the district court’s finding that the fraud-related losses were in excess of $100 million.\(^{29}\)

In examining Olis’s sentence, the court noted that *Dura Pharmaceuticals*’ principles provided useful guidance for determining criminal responsibility.\(^{30}\) The court looked to these principles for guidance because they “furnish[] the standard of compensable injury for securities fraud victims and because [they are] attuned to stock market complexities.”\(^{31}\) The Fifth Circuit vacated Olis’ sentence, finding that the district court did not take into account “the impact of extrinsic factors on Dynegy’s stock price decline” in its

---

\(^{27}\) *United States v. Olis*, 429 F.3d 540 (5th Cir. 2005).

\(^{28}\) *Id.* at 541.

\(^{29}\) *Id.* at 542, 545 (“The most significant determinant of Olis’ sentence is the guidelines loss calculation. By the district court’s reasoning, this added twenty-six levels to his base offense level and alone placed Olis in a punishment range exceeding fifteen years’ imprisonment.”).

\(^{30}\) *Id.* at 546.

\(^{31}\) *Id.*
approach to the loss calculation. Accordingly, the Fifth Circuit remanded to the district court to reconsider the U.S. Sentencing Guidelines, including a recalculation of the loss caused by Olis’s conduct. On remand, the district court sentenced Olis to 72 months in prison; 220 months less than his original sentence.

C. The Second Circuit’s Decision in United States v. Rutkoske

In 2007, the Second Circuit reached a similar conclusion in United States v. Rutkoske. David Rutkoske was convicted of securities fraud and conspiracy to commit securities fraud. He was sentenced to 108 months in prison based on a U.S. Sentencing Guidelines range determined from a total offense level of 31. The offense level included a 15-level enhancement for loss of more than $10 million. Rutkoske objected to the loss calculated by the presentence report, which had been based on the trial testimony of a National Association of Securities Dealers expert.

Like the Fifth Circuit, the Second Circuit noted that Dura Pharmaceuticals’ principles provided useful guidance for determining criminal responsibility. The Second Circuit saw “no reason why considerations relevant to loss causation in a civil fraud case should not apply, at least as strongly, to a sentencing regime in which the amount of loss caused by a fraud is a critical determinant of the length of a defendant’s sentence.” The court acknowledged that the U.S. Sentencing Guidelines allowed for a “reasonable estimate” of loss and that such allowance remained pertinent. However, the district court failed to at least approximate the amount of loss caused

---

32 Id. at 548-49.
33 Id. at 549.
35 United States v. Rutkoske, 506 F.3d 170 (2d Cir. 2007).
36 Id. at 174.
37 Id. (The 15-level enhancement had the effect of adding 87 months onto Rutkoske’s sentence).
38 Id.
39 Id. at 179.
40 Id.
41 Id.
by the fraud absent other factors relevant to a decline in the company’s share price. Accordingly, the Second Circuit remanded to the district court to recalculate the amount of loss, for both sentencing and restitution purposes.

III. THE NINTH CIRCUIT DECLINES TO APPLY LOSS CAUSATION PRINCIPLES IN CONNECTION WITH CRIMINAL SECURITIES FRAUD SENTENCING

In United States v. Berger, the Ninth Circuit explicitly declined to follow the Fifth and Second Circuits’ extension of Dura Pharmaceuticals’ principles to criminal sentencing. Richard Berger, President, Chief Executive Officer, and Chairman of the Board of Craig Consumer Electronics, Inc. (Craig), was convicted of 12 counts of bank and securities fraud for misrepresenting his company’s fiscal viability and financial condition in connection with his company’s IPO. Craig was required to restate its past earnings in the year following Berger’s misrepresentation as a result of an audit of the company’s accounting records. In the months following the restatement, the company’s stock price fell from $4.99 to $0.99 per share.

The district court initially sentenced Berger to only six months imprisonment due to its belief that “controlling authority prohibited it from applying any sentencing facts not found by the jury.” On appeal, the Ninth Circuit vacated Berger’s sentence and remanded to the district court for resentencing in light of United States v. Booker. On remand, the district judge sentenced Berger to 97 months in prison. This sentence was on the low end of a U.S. Sentencing Guidelines range of 97 to 121 months which was based

---

42 Id. at 180.
43 Id.
44 United States v. Berger, 587 F.3d 1038, 1042-43 (9th Cir. 2009).
45 Id. at 1040.
46 Id. at 1041.
47 Id. at 1040.
48 Id.
49 Id. at 1040.
50 Id.
51 Id.
on an offense level that included a 14-level sentencing enhancement for a calculated loss of $5.2 million. On his second appeal, Berger argued that the district court erred by not employing the *Dura Pharmaceuticals* approach in calculating loss.

While recognizing that two other circuit courts had applied *Dura Pharmaceuticals*’ principles to the calculation of loss in criminal sentencing, the Ninth Circuit held that the primary rationale behind the *Dura Pharmaceuticals* decision did not apply in criminal cases. The Ninth Circuit reasoned that the Supreme Court in *Dura Pharmaceuticals* was “concerned principally with the plaintiff’s ability to show that he suffered actual loss caused directly—and exclusively—by the defendant’s fraudulent misrepresentation.” This is in contrast to criminal cases, where the court is concerned with the loss to society as a whole as opposed to a particular person’s loss. Therefore, even if an individual’s loss cannot be directly linked to the fraud, there could still be general loss to society based on the defendant’s fraud.

In addition, the court found that the application of *Dura Pharmaceuticals* ran contrary to the U.S. Sentencing Guidelines. Specifically, application of *Dura Pharmaceuticals*’ loss causation principles to criminal sentencing enhancements would conflict with “Congress’s clear endorsement” of the overvaluation loss measurement method. By rejecting the application of *Dura Pharmaceuticals* in criminal sentencing, the Ninth Circuit relied on its prior decision in *United States v. Hicks* to find that “a defendant’s sentence [must be based on the] harm that resulted from the acts or omissions of the defendant.”

---

52 Id.
53 Id. at 1042.
54 Id. at 1043.
55 Id. at 1044.
56 Id.
57 Id.
58 Id. at 1045.
59 *United States v. Hicks*, 217 F.3d 1038 (9th Cir. 2000).
60 *Berger*, 587 F.3d at 1044 (quoting *Hicks*, 217 F.3d at 1048).
IV. IMPLICATIONS OF THE NINTH CIRCUIT’S DECISION IN UNITED STATES V. BERGER

The amount of loss caused by securities fraud can be a key amplifying factor at sentencing; it has the potential to increase the offense level by as many as 30 levels.61 For example, in Olis, the defendant’s base offense level was increased by 26 levels due to a loss calculation of $105 million.62 The large impact of that loss calculation lessens the impact of more relevant issues, such as the actual motive of the perpetrator, extenuating circumstances, and the personal benefit received by the defendant.63 Instead, these important issues have been completely replaced by complex loss calculations.

Also, greater uncertainty exists under the Ninth Circuit’s decision in Berger because the U.S. Sentencing Guidelines provide little guidance to courts with respect to how loss should be calculated. Courts are expected to apply the greater of actual loss or intended loss in its determination of loss.64 In addition, courts need only make a reasonable estimate of loss.65 Since numerous theories have developed to calculate loss, a reasonable estimate of loss may differ depending on the sentencing court. Furthermore, these different methods will likely be upheld in the Ninth Circuit, allowing for a broad range of criminal sentences arising from similar conduct.

In addition, the Ninth Circuit’s decision in Berger will likely have an effect on pretrial negotiations among prosecutors and criminal securities fraud defendants. These defendants will face the tough choice between entering into a plea agreement with a predefined sentence or risk receiving a potentially greater sentence based on the sentencing court’s calculation of loss under Berger. However, within the Second and Fifth Circuits, defendants will likely have a greater incentive to go to trial rather than negotiate a plea, because they will be less at risk of incurring a large sentence increase due to the sentencing court’s loss calculation.

---

62 United States v. Olis, 429 F.3d 540, 543 (5th Cir. 2005).
64 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3(A) (2010).
65 Id. at § 2B1.1 cmt. n.3(C) (2010).
CONCLUSION

The Ninth Circuit’s decision in Berger has set up a circuit conflict among the Second, Fifth, and Ninth Circuits. This may lead to uncertainty as to the calculation of loss in criminal securities fraud sentencing throughout the country. Defendants in the Ninth Circuit and perhaps other circuits may now be at the mercy of prosecutors to reach a plea agreement before trial to avoid the nearly exponential sentence increase that may come with the calculation of market loss at sentencing. For those choosing to go to trial, their lawyers must attempt to persuade sentencing courts to adopt conservative approaches to U.S. Sentencing Guidelines calculations to avoid any significant increase to the defendant’s offense level. Given the split on this issue, it may be necessary for the Supreme Court to clarify whether civil loss causation principles should be applied in criminal securities fraud cases. Until this issue is resolved by the Supreme Court, criminal securities fraud defendants will have a tough choice to make: whether to settle with prosecutors before trial or risk a large sentence increase due to market loss calculations.
GIMME A BREKKA!: DECIPHERING “AUTHORIZATION” UNDER THE CFAA AND HOW EMPLOYERS CAN PROTECT THEIR DATA

Amber L. Leaders*

© Amber L. Leaders

Cite as: 6 Wash J.L. Tech. & Arts 285 (2011)
http://hdl.handle.net/1773.1/1036

ABSTRACT

Federal circuit courts offer conflicting interpretations of when an employee violates the Computer Fraud and Abuse Act (CFAA) by accessing an employer’s computer system without authorization. Enacted originally as an anti-hacker statute, the language of the CFAA proves ambiguous when courts attempt to apply its sanctions to individuals given access to a computer (such as an employee by an employer). Circuit Courts have interpreted the statute differently, generally applying one of two theories to reach their interpretations: (1) agency theory; or (2) looking to the plain language of the statute and the rule of lenity. These differing interpretations have resulted in varying outcomes when employers seek to sanction employees for violating the Act. Employers face tough questions about when and how to seek sanctions when employees potentially violate their rights of computer access. This Article takes an in-depth look at the varying interpretations among the circuits and considers a number of district court cases and their application of the CFAA.

* Amber L. Leaders, University of Washington School of Law, Class of 2011. Thank you to my student editor, Jeff Doty, for his enduring patience and thoughtful critiques and to my faculty advisor, Anita Ramasastry, for her valuable feedback and guidance.
INTRODUCTION

The Computer Fraud and Abuse Act (CFAA)1 both criminalizes unauthorized access to certain private computer systems and allows parties harmed by such access to bring civil actions for compensatory damages and injunctive relief. With the growing use of computers by employees at all levels, however, companies increasingly face the loss of sensitive data through internal acts – violations by their own workers. The language of the CFAA is ambiguous about whether the Act should apply to these internal violators. Thus, federal circuits have split on what it means to be without or to exceed authorized access under the CFAA.

The principle interpretations come from the U.S. Courts of Appeals for the Seventh and the Ninth Circuits.2 In International Airport Centers L.L.C. v. Citrin,3 the Seventh Circuit used agency law to determine when authorization by an employee begins and ends; under this interpretation, an employee violates the CFAA when the agency relationship is severed and thus authorization is constructively rescinded. In contrast, the Ninth Circuit in LVRC Holdings LLC v. Brekka4 interpreted the statute according to its plain language to determine when an employee lacks authorization. The

2 See Int’l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); LVRC Holdings LLC, v. Brekka, 581 F.3d 1127 (9th Cir. 2009).
3 Citrin, 440 F.3d at 423.
4 Brekka, 581 F.3d at 1134.
Ninth Circuit finds a violation of the CFAA only when no authorization has ever been given or when authorization has affirmatively been rescinded by an employer.5 For any employer seeking damages or injunctive relief against a rogue employee, it will be important to consider the branches of interpretation as well as the many offshoots in each of the district courts. This Article examines the Citrin and Brekka decisions and considers cases from the district courts to determine how these varying analyses affect employers faced with the threat of computer-system breaches.

I. THE ORIGIN AND PURPOSE OF THE CFAA

The difficulty in interpretation of the CFAA arises from the origin of the statute. Enacted in 1984 to help the federal government prosecute computer crimes, Congress designed the CFAA to target hackers who “break in” to systems.6 But the CFAA has grown from protecting only “federal interest computers” to guarding any “protected computer.”7 Further, the original incarnation was solely a criminal statute, but the scope of the CFAA has gradually expanded through legislative enhancements to include a private right of action.8 That private action allows an individual to seek civil remedies when he or she has suffered loss or damages as a result of someone else’s improper access.

Section 1030 prohibits five categories of conduct: (1) theft of computer data; (2) unauthorized access with intent to defraud;
(3) unauthorized access resulting in destruction; (4) trafficking in computer passwords; and (5) extortion by threat of damage to a computer. All but the fifth category contain the qualifying language “without authorization” or “exceeds authorized access.” These two phrases are the root of the dispute between the various circuits.

The CFAA states in relevant part that whoever “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information contained in a financial record of a financial institution, or of a card issuer … or contained in a file of a consumer reporting agency on a consumer” commits a federal crime. Courts employ different methods in applying the language of “without authorization” or “exceeds authorized access” to a computer.

Because the original purpose of the CFAA was to keep third parties from illegally accessing others’ computers and information, the language regarding authorization can be unclear when applied to an employee who has been given a degree of authorization by the employer. Courts have struggled to apply this anti-hacker statute when the offender is not a third party but someone who has been given access to the computer, such as an employee.

II. THE SPLIT BETWEEN CITRIN AND BREKKA

The circuit split centers on when employees have authorization to access computer systems. The Seventh Circuit uses agency law to define the boundaries of authorization. In Citrin, it held that when an employee violates his or her fiduciary duty of loyalty to the employer, all access authorization ceases. The Ninth Circuit recently offered an alternative interpretation of the same statutory language. Using the “plain language” of the CFAA, that court determined that the CFAA has narrower parameters for what constitutes a violation. District courts have varied in their application of the two interpretations, with most following the Ninth Circuit’s reasoning.

9 Id.
11 Int’l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006).
12 LVRC Holdings LLC, v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).
13 Id.
A. The Seventh Circuit and Agency Law

In Citrin, the Seventh Circuit applied agency theory to interpret the vague language regarding authorization in the CFAA. Citrin was an employee of International Airport Centers (IAC), which loaned Citrin a laptop for work. He decided to go into business for himself, in breach of an employment contract. Before departing, Citrin deleted numerous files that implicated his intent to develop a competing business using IAC’s data from his loaned laptop. Beyond deleting the files, Citrin utilized a special program designed to overwrite deleted files, thus making them unrecoverable. He had been given access by IAC to the computer and to the files. IAC alleged the deleted files implicated Citrin and that was why they were deleted. The company sought civil remedies against Citrin under the CFAA for accessing data without authorization and for wrongfully transmitting information.

The Citrin court held that an employee’s authorization to access a computer ends for purposes of the CFAA when the employee violates her duty of loyalty to the employer. Under agency theory, an employee violates that duty when he or she determines to act wrongfully or break loyalty (such as by taking another job) with the employer. The court determined that Citrin violated his fiduciary duty of loyalty to IAC and therefore acted “without authorization” in accessing the files. This decision was the primary appellate interpretation of the authorization language in the CFAA until the Ninth Circuit’s decision in Brekka.

14 Citrin, 440 F.3d at 420.
15 Id. at 419.
16 Id.
17 Citrin, 440 F.3d at 420-21.
19 Id.
20 The First Circuit also considers the issue, but offers a similar interpretation as the Seventh Circuit and the Citrin case is the one generally cited as the primary authority. See Nick Akerman, Time to Review Corporate Computer Policies, NAT’L L.J. (Feb. 3, 2010), http://computerfraud.us/files/2010/03/Time-to-Review-Computer-Policies-v1.pdf.
B. The Ninth Circuit and Plain Language Interpretation

In September 2009, the Ninth Circuit decided Brekka, another case involving an employee’s improper use of company files. The Ninth Circuit was “unpersuaded by [the] interpretation” of the Seventh Circuit.21 Instead, the court considered the plain language of the statute and the rule of lenity for criminal or quasi-criminal statutes.22 LVRC Holdings employed Brekka to manage one of its treatment facilities. As part of this position, Brekka received access to the computer system and full access to any files or records. During his employment, Brekka travelled between his work in Nevada and his home in Florida. He often transmitted files between his work and home computers. He eventually decided to start his own business and dumped a number of files, including confidential information, from his work computer to his home laptop. LVRC Holdings sought civil damages against him for violation of the CFAA.

The Brekka court first noted that the CFAA is primarily a criminal statute, although Brekka was a civil case,23 and determined that as a criminal statute the rule of lenity should be applied in interpreting any ambiguity of language.24 The rule of lenity mandates that courts interpret ambiguous criminal statutes in favor of the defendant in order to avoid unexpected burdens.25 According to the court, the “rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government.”26 The court specifically cited Citrin and stated that applying agency theory in these cases would lead to confusion for defendants because such an interpretation is not implied by the plain language of the statute.27

21 Brekka, 581 F.3d at 1134.
22 Id. at 1134-35.
23 The CFAA is a criminal statute, but it provides civil remedies in addition to criminal penalties. Fishman and McKenna, Wiretapping and Eavesdropping §26:1 (2010).
24 Brekka, 581 F.3d at 1134.
25 Id.
26 Id. at 1135(citing United States v. Romm, 455 F.3d 990, 1001 (9th Cir. 2006)).
27 Id.
The Brekka Court then considered the plain language of the statute to determine the meaning of authorization. The court defined “authorization” to access a company’s computer as “when the employer gives the employee permission to use it.” The court reasoned that the CFAA’s plain language says nothing about an employee’s fiduciary duty of loyalty. Authorization begins and ends with the employer, not the employee, under this view. An employee acts without authorization only if the employer never gives permission or affirmatively rescinds permission. The court determined that Brekka was not liable under the CFAA because the LVRC had authorized his access to the computer. In the court’s view, this was not “without authorization” as the statute requires.

The court further opined that Brekka could not have violated the CFAA under “exceeds authorized access” because he only accessed the computer as the company had allowed. The CFAA addresses access, not use, according to the Ninth Circuit. What the employee does with materials after properly accessing them does not bring the employee’s actions under the sanctions of the CFAA.

The Ninth Circuit is the first federal appellate court to apply this reasoning. However, the Brekka Court’s rationale is not new. Prior to the Brekka opinion, district courts had applied similar logic when interpreting the terms “authorization” and “authorized access.”

The interpretations from the Citrin and Brekka decisions provide the guideposts for other interpretations of the CFAA. Other circuits have interpreted the statute similarly, with some minor variation.

28 Id.
29 Id. at 1133.
30 Id. at 1135.
31 See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001)(supporting the Citrin analysis, but noting use of “scraper” program “exceeded authorized access,” assuming program's speed and efficiency depended on breach of confidentiality agreement with former employer); ReMedPar, Inc. v. AllParts Medical, LLC, 683 F.Supp.2d 605, 613 (M.D.Tenn 2010)(following the Brekka reasoning, but attaching legislative history analysis as well); Bro-tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378, 407 (E.D. Pa. 2009)(supporting the Brekka reasoning, but noting that whether an employee who had deleted emails from his company computer before discharge had exceeded authorized access is a question of fact for a jury); Cenveo, Inc. v. Rao, 659 F. Supp. 2d 312, 317 (D. Conn. 2009)(stating transmission of confidential information via computer is not enough, but can only exceed access if the information accessed was in the computer).
The reasoning of Brekka has been more widely adopted and can be found in district court cases from the Second, Third, Fourth, Sixth, Eighth, and Tenth Circuits. Most of these apply an almost identical analysis to that of the Brekka case, though the Second and Fourth Circuits have slight variations. In these cases, courts often find an employee is without authorization only when he or she never received access to particular data or systems. Once an employee receives access to a system, an employer has little recourse under the Ninth Circuit interpretation of “without authorization.”

C. Beyond Citrin and Brekka: The Fifth and Eleventh Circuits’ Interpretations of the CFAA

Two circuit court decisions following Brekka further outline the nuances of applying §1030(a)(2)(B), particularly to employees who exceed authorized access. Both decisions highlight the importance of the employee’s knowledge. The Fifth Circuit in U.S. v. John noted that “an authorized computer user ‘has reason to know’ that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme” and thus violates the CFAA by acting. The Eleventh Circuit ruled that notice to the employee of his access limits could be dispositive in determining whether authorization was exceeded. Both decisions seem to distinguish, rather than dispute, the holding in Brekka.

In John, the Fifth Circuit considered the “exceeds authorization” language of the CFAA. The court held that employers have broader protections against rogue employees than under the Ninth Circuit’s interpretation. Unlike many of the other cases, the actions of the

32 Though this Article uses Brekka as a guidepost, many of the referenced district court cases applied the same line of reasoning as Brekka prior to the Brekka decision.
33 Cenveo, 659 F. Supp. 2d at 316 (noting a distinction where accused did not access information “in a computer”); Werner-Masuda, 390 F.Supp.2d at 499 (noting distinction where the act is unauthorized disclosure of information rather than unauthorized access to information).
34 U.S. v. John, 597 F.3d 263 (5th Cir. 2010).
35 John, 597 F.3d at 273.
36 United States v. Rodriguez, 628F.3d, 1258, 1260 (11th Cir. 2010).
37 John, 597 F.3d at 273-73.
employee in *John* were criminal both under the CFAA and separate criminal fraud statutes. The employee accessed employer information and bank account records and used the information to defraud customers. Furthermore, the employer told the defendant that such access was prohibited and beyond the scope of what was authorized. The court determined that the defendant’s access exceeded authorization, stating that access “to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded.”

The Fifth Circuit drew an important distinction from the *Brekka* case; the court noted that “the Ninth Circuit may have a different view” on how it interpreted the “exceeds authorization” language. In *Brekka*, the court had determined that if an employer had not affirmatively rescinded authorization, an employee “would have no reason to know” that personal use might also violate the CFAA. The *John* court stated that in its case, the reasoning that the employee “had no reason to know” did not apply.

The violator in *John* had not only accessed employer data but had done so in “furtherance of a criminally fraudulent scheme.” The Fifth Circuit stated that “when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer’s policies and is part of an illegal scheme, it would be ‘proper’ to conclude that such conduct ‘exceeds authorized access’ within the meaning of § 1030(a)(2).” This interpretation of the phrase “exceeds authorized access” broadens the application of the CFAA beyond what the Ninth Circuits and other courts apply, but stops short of the employer-friendly holding in *Citrin*. Rather than providing blanket protection for employees given access by the employer, the Fifth Circuit imposes an important limitation on employees who violate employer policies and do so as part of an illegal act. This gives employers some remedies against gross

---

38 *Id.* at 272.
39 *Id.*
40 *Id.*
41 *Id.* at 273 (citing *Brekka*, 581 F.3d at 1134).
42 *Id.*
43 *Id.*
44 *Id.*
violations by employees – even employees previously granted access – but does not extend to employees who merely disregard the employer’s expectation of loyalty.

The Eleventh Circuit decided in *U.S. v. Rodriguez* that notice to the employee that accessing information, otherwise normally authorized, outside the scope of normal business reasons was prohibited met the plain language of the CFAA. The employer, Teleservice, had advised Rodriguez that accessing the personal information databases was only authorized for business reasons. Any access outside of that scope was prohibited. Furthermore, Rodriguez readily admitted that he was aware of this policy and had accessed “things that were not authorized.”

The court distinguishes its holding from both the *Brekka* and *John* decisions. The court states that this case differs from *Brekka* in that the employer there had not provided any such notice to the employee regarding the prohibited access. The court distinguishes *John* on the grounds that Rodriguez’s lack of criminal use of the information (as required by *John*), “is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access.” The court does not reach the *John* standard because, unlike in *John*, Rodriguez exceeded his authorized access by violating a known policy of the employer.

### III. WHAT CAN EMPLOYERS DO? A LOOK AT PRACTICAL SOLUTIONS

Employers should be careful to consider whether an employee acted without authorization or exceeded authorized access because circuit courts interpret the terms of the CFAA differently. Courts that follow the *Citrin* approach favor a broader acceptance of contractually setting up boundaries for authorization, for instance through confidentiality, employment, and noncompete agreements. In jurisdictions following *Citrin*’s agency law approach, employers have

---

45 United States v. Rodriguez, 628F.3d, 1258, 1263 (11th Cir. 2010).
46 *Id.* at 1260.
47 *Id.* at 1262.
48 *Id.* at 1263
49 *Id.*
more power to set up the boundaries that they want individual employees to follow. Specificity in employment agreements is not as crucial because of the loyalty requirements under agency theory that give employers a remedy regardless. But a best practice will be to make employment agreements specific enough to outline employee expectations of what could break the agency relationship. The more important issue in determining liability is whether an employee acted disloyally towards the employer or acted with wrongful purpose.

Under the Brekka analysis or similar interpretation, employers should limit the access of lower-level employees and expand access only when necessary. The larger question for employers under the Brekka analysis is what to do with those employees that require extensive access to data and systems. Those types of employees leave employers most vulnerable to breaches of confidentiality and noncompete agreements. Under Brekka, an employer’s recourse may be limited under the CFAA. Even having confidentiality agreements, employment agreements, and computer policies does not always save employers in these circuits.

The John court sets forth a middle ground. An employer cannot use the “without authorization” language of the CFAA as a sword to parry employees already given access. But an employer may have some remedies under “exceeds authorized access.” An employee who uses information obtained from a computer system as part of a criminal scheme when subject to a detailed employee computer-use policy that states exactly when an employee exceeds access probably violates the CFAA.

Rodriguez goes one step further, stating that a detailed policy by the employer and a demonstration that the employee had knowledge of that policy is enough to show access was not authorized or exceeded authorization under the CFAA. Under those circumstances, whether an employee planned to use the information as part of a criminal scheme is irrelevant. Knowledge and violation of the employer’s policy can be sufficient to demonstrate the employee exceeded authorized access.

CONCLUSION

Employers should strive to limit computer access to employees and to clearly communicate computer-use policies to those with
access. The courts generally apply the CFAA in favor of employees. However, some circuits are giving employers a fighting chance. The Fifth and Eleventh Circuit rulings give more ground to employers. The best defense for employers is not to rely on the CFAA as a remedy but to limit access of employees to sensitive data and to be clear about what those limits are through detailed policies, computer-use agreements, and records demonstrating employees’ knowledge of those policies.
ABSTRACT

Copyright management information (CMI), defined by the Digital Millennium Copyright Act (DMCA), is information conveyed with a copyrighted work that identifies the owner and nature of that copyright. Although the DMCA prohibits the knowing removal of CMI under 17 U.S.C. § 1202(b), district court decisions relating to CMI are split on whether its provisions apply only to digital forms or also extend to non-digital CMI conveyance. This Article describes the current state of CMI jurisprudence and the expected effects of possible interpretive outcomes.

TABLE OF CONTENTS

Introduction .................................................................298
I. The DMCA and CMI .........................................................299
II. CMI’s Possible Meanings Under the DMCA....................300
III. DMCA Context-Sensitive Interpretations of CMI.............301
IV. Broader Interpretations of CMI: General Applicability? ....304
V. Practical Implications of § 1202 Construction .................305
   A. Availability of § 1203 Damages .......................306
   B. Relationship Between DMCA CMI Requirements and

*  Susuk Lim, University of Washington School of Law, Class of 2011. My sincere thanks to Professor Jane Winn, attorney Brian Esler of Miller Nash LLP, and student editors Stephanie Holmes, Kendra Rosenberg, and Homer Hsu for their invaluable input and guidance.
INTRODUCTION

The Digital Millennium Copyright Act (the Act) protects copyright management information (CMI) placed by a copyright’s owner. The Act generally defines CMI as “information conveyed in connection with [copyrighted works] . . . including in digital form,” that identifies the owner and nature of the copyright itself. However, the statutory wording leaves open questions about whether the protections are specific to digital CMI in digital media, digitally created CMI in either digital or analog media, or all CMI in media.

Earlier CMI-related decisions split between two interpretive camps. The narrower interpretation construed CMI protection strictly within the context of the Act’s overarching legislative purpose. It therefore limited CMI protection to digital measures, such as copyright information embedded in software as a part of a larger digital rights management (DRM) system. Other courts favored a broader approach and were willing to expand the CMI protection beyond digitally stored CMI to digitally placed CMI, such as digitally embedded watermarks in printed photos. Courts following the latter approach avoided foreclosing the Act’s applicability to entirely analog CMI.

Two recent district court decisions, McClatchey v. Associated Press and Associated Press v. All Headline News, endorse an even broader interpretation of the Act’s CMI provisions. Both decisions explicitly extend the reach of the Act’s CMI provisions beyond digital forms of transmission or conveyance to fully analog CMI manifestations. This interpretation has potentially significant effects.

on copyright enforcement, some of which are detailed below.

Absent an authoritative Supreme Court opinion, the split remains. This Article surveys these cases, formulates a unified picture of the Act’s CMI protections, and concludes with practical suggestions on how to best assess the validity of a CMI claim under the Act.

I. THE DMCA AND CMI

The Act is a statutory implementation of two treaties with the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, both signed in 1996. The Act broadly addresses the protection of digital production and dissemination of copyrighted technological and technologically created works. Two of the Act’s many mandates are protection against circumvention of technological copyright measures and preservation of CMI. The former, codified in § 1201, targets a specific class of devices and services, but § 1202, dealing with CMI, only imposes liability for certain acts.

Sections 1201 and 1202, known as the “anti-circumvention” provisions, are the codification of Articles 11 and 12 of the 1996 WIPO Copyright Treaty, which requires parties to “provide adequate legal protection . . . against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights” and to provide “effective legal remedies against any person knowingly . . . remov[ing] or alter[ing] any electronic rights management information without authority.” The treaty itself is notable because it specifically mentions the protection of electronic rights management.

---

8 Id. § 1202.
10 Id. art. 12 para. 1.
The language in §§ 1201 and 1202 differs subtly from that of the treaty. Subject to several incidental exceptions, § 1201 bans the “circumvention of technological measure[s] that effectively control access” to protected works. Like the remainder of the Act, the section specifically addresses “technological measures,” not other measures more broadly covered by general copyright doctrine. This language reflects Article 11. However, § 1202, which covers CMI and implements Article 12, contains no such wording. Courts disagree whether CMI, as protected by § 1202, must be by definition a “technological measure” within the meaning of § 1201 or whether the textual exclusion of technological requirements implies a broader definition. This Article analyzes whether these two provisions should be read in isolation or together as a broader statutory scheme.

II. CMI’S POSSIBLE MEANINGS UNDER THE DMCA

Section 1202 protects eight distinct categories of information as CMI, if used “in connection with copies . . . performances or displays of a work.” The categories include: (1) the work’s title; (2) its author; (3) its copyright owner; (4) names of performers in non-audiovisual; non-broadcast work; (5) names of writers, performers, and directors in audiovisual, non-broadcast work; (6) terms and conditions for the work’s use; (7) links, numbers, or codes referring to CMI; and (8) any additional data properly added to the definition by administratively promulgated regulation.

Data belonging to any of these categories may not be removed, altered, or falsified if they are conveyed in conjunction with a copied work. Data not falling into one of § 1202’s eight CMI categories is not protected under the Act’s provisions but may be subject to other laws, such as unfair trade. Section 1202 claims require both intent to remove or alter the CMI and a showing of actual infringement resulting from the removal or alteration. Violations of § 1202 are...
punishable by actual and fixed statutory damages under § 1203.\textsuperscript{16} Criminal penalties apply to willful and commercially exploitative violators.\textsuperscript{17}

The debate about whether CMI protected by § 1202 must be a “technological measure” centers on § 1202’s inapt wording and poorly documented legislative history. Section 1202 contains no mention of other Act-created provisions and includes the phrase “including in digital form” when defining CMI for the purpose of § 1202. This implies that § 1202’s definitions have a broader reach than merely that of the technological realm.

Because it is part of the Act, it is also possible to read § 1202 to target only technological copyright protection methods and digital methods of conveying CMI. This would rule out a broader interpretation including traditional copyright management, such as copyright notices in textbooks. The Act was enacted with the stated goal of creating “the legal platform for launching the global digital on-line marketplace for copyrighted works” and to “make digital networks safe places to disseminate and exploit copyright materials.”\textsuperscript{18} It would follow that the Act’s provisions should be interpreted in the context of its legislative purpose. The first courts to consider the issue espoused this context-sensitive view.

### III. DMCA Context-Sensitive Interpretations of CMI

In 2006, a New Jersey district court provided the first detailed interpretation of § 1202 in \textit{IQ Group v. Wiesner}.\textsuperscript{19} In \textit{IQ Group}, the defendant, Wiesner Publications, redistributed an online advertisement for a client shared with the plaintiff, IQ Group. In so doing, it removed an embedded logo belonging to the plaintiff and replaced it with its own. The court considered the breadth of § 1202’s coverage in light of its statutory construction, the state of jurisprudence within the copyright field, and the statute’s legislative

\textsuperscript{16} 17 U.S.C. § 1203(c) (2006) (note that both § 1201 and § 1202 are mentioned directly).
\textsuperscript{17} \textit{Id.} § 1204(a).
Though it conceded that a literal reading of the statute implied a broad application, the court determined that the statute should be subject to a “narrowing interpretation” that only protects CMI functioning “as a component of an automated copyright protection or management system.” The court held that § 1202 should not be “construed to cover copyright management performed by people, which is covered by the Copyright Act.” Under this standard, the court found insufficient evidence that the logo served as a component of automated copyright protection or management and granted summary judgment to the defendants.

The court reasoned that while authors traditionally used copyright law to protect their legal rights, modern technological measures have increasingly displaced law in controlling access to works. It noted that the purpose of the Act was to protect those technological measures rather than the copyrights themselves.

Under this standard, the court found insufficient evidence that the logo served as a component of automated copyright protection or management and granted summary judgment to the defendants.

The court reasoned that while authors traditionally used copyright law to protect their legal rights, modern technological measures have increasingly displaced law in controlling access to works. It noted that the purpose of the Act was to protect those technological measures rather than the copyrights themselves.

Finally, the court noted that this narrow interpretation made § 1202 consistent with § 1201, as

---

20 Id. at 593.
21 Id. at 597.
22 Id.
24 See id. at 594-97.
26 *IQ Group*, 409 F. Supp. 2d. at 596.
well as Chapter 12 as a whole.

About one year later, a California district court largely followed IQ Group’s reasoning in Textile Secrets v. Ya-Ya, though it reached a somewhat less definitive conclusion. The case involved an allegedly copied textile design. The plaintiff, Textile Secrets, registered a copyright for a textile of its own design. The defendant, a high-end clothing designer named Ya-Ya Brand Inc., had allegedly taken sample yardage of the fabric provided by the plaintiff and incorporated it into its own clothing after removing tags indicating the design’s registered ownership. Textile Secrets argued that Ya-Ya’s removal of the tag constituted a violation of § 1202.

Applying basic principles of statutory construction, the court reached a similar initial result to IQ Group and determined that § 1202 must be construed in light of Chapter 12 as a whole and as a part of the Act’s Title I. A literal reading, as also noted by IQ Group, would result in § 1202’s applicability “wherever any author has affixed anything that might refer to his or her name.” It found this interpretation impracticable within the context of the Act’s structure, thus justifying an inquiry into § 1202’s legislative history.

The Textile Secrets court also assessed the White Paper and subsequent legislative history and concurred with IQ Group’s narrowed interpretation of § 1202. However, the court noted in dictum that it did “not find it necessary to define the scope . . . [as] only [applying] to copyright management information that functions ‘as a component of an automated copyright protection or management system.’” Thus, unlike in IQ Group, the Textile Secrets court construed § 1202 as possibly applying to technological measures that directly or effectively control access to work, not solely to components of automated copyright management systems.

Both cases interpreted § 1202 narrowly; neither court imputed tangible or non-digital forms of copyright information into § 1202’s

---

28 Id. at 1188.
29 Id. at 1192-93.
30 Id. at 1195.
31 Id. (quoting IQ Group, 409 F. Supp. 2d at 593).
32 Id. at 1203, n. 18.
33 Id. at 1202-03.
scope. But the dictum in Textile Secrets was a harbinger for a wholesale interpretive change.

IV. BROADER INTERPRETATIONS OF CMI: GENERAL APPLICABILITY?

Some recent district court decisions have broadened § 1202’s applicability. Shortly after Textile Secrets, the district court of the Western District of Pennsylvania held in McClatchey v. Associated Press that § 1202 also applies to non-digital information.34 Plaintiff McClatchey took and subsequently registered a copyright for a photo of Flight 93’s crash during the events of September 11, 2001. The defendant, Associated Press (AP), allegedly redistributed the photo, replacing McClatchey’s copyright information with its own.

In denying summary judgment for the AP, the court chose to interpret § 1202 broadly based on the face of the statute; specifically, it pointed to § 1202(c)’s assertion that “copyright management information” includes “any” information falling within § 1202’s categories, “including in digital form.”35 The court reasoned that to “avoid rendering those terms superfluous, the statute must also protect non-digital information.”36 It noted that the usage of a computer to add copyright management information already constitutes the use of a digital or technological device to add CMI.37 Unlike the IQ Group or Textile Secrets courts, however, the McClatchey court took a strictly textual approach to § 1202 interpretation and declined to participate in a detailed analysis of the legislative history.

The McClatchey court used language in IQ Group to justify its position. Part of IQ Group’s test for CMI protection is a determination of whether the CMI “functioned as a component of an automated copyright protection system.”38 Whereas in IQ Group this determination was meant to cabin § 1202 strictly to CMI used as part of an automated management system, the McClatchey court

34 McClatchey, 2007 WL 776103.
35 Id. at *5.
36 Id.
37 Id.
understood this language to encompass the process of using software to place copyright information on analog works, such as pictures.\textsuperscript{39} This construction broadened the reach of § 1202 significantly.

Another recent case involving CMI also endorsed a broad interpretation of § 1202, but rejected \textit{IQ Group}’s and \textit{Textile Secrets}’ approaches altogether. In 2009, a New York district court in \textit{Associated Press v. All Headline News} found § 1202’s language clear enough on its face to bar any inquiry into its legislative history.\textsuperscript{40} The plaintiff, AP sued defendant All Headline News for misappropriating news from the AP’s ticker and replacing the AP’s copyright notice with its own. The \textit{Associated Press} court declined to follow the rationales of the decisions in \textit{IQ Group} and \textit{Textile Secrets}, stating that Second Circuit rules of statutory construction barred them from inquiring into legislative history “‘to cloud statutory text that is clear’ even if there are ‘contrary indications in [that] history.’”\textsuperscript{41} The court then used similar logic as the \textit{McClatchey} court in determining that no inquiry into the methods or nature of the CMI removal was necessary because the statute plainly contemplated even non-digital alteration of analog data to be within its scope.\textsuperscript{42} Unlike \textit{McClatchey}, however, it found no reason to use language from \textit{IQ Group} to justify its decision, instead reading the statute itself as being applicable to all kinds of copyright information, whether analog or digital. It notably found no mention of “technological measures of automated systems” within the statute itself and thus saw no reason to limit the section’s applicability.\textsuperscript{43}

\section*{V. Practical Implications of § 1202 Construction}

It is unclear how this interpretive split will be resolved, though no recent trial or appellate court has rejected the textualist approach endorsed by \textit{McClatchey} and \textit{Associated Press}. A narrow § 1202 interpretation implies that CMI protection provisions are treated separately from general copyright law. A broad § 1202 interpretation,

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{39} McClatchey, 2007 WL 776103, at *5.
\item \textsuperscript{40} Associated Press v. All Headline News, 608 F. Supp 454 (S.D.N.Y. 2009).
\item \textsuperscript{41} Id. at 461-62 (quoting Ratzlaf v. U.S., 510 U.S. 135, 147-48 (1994)).
\item \textsuperscript{42} Id. at 462.
\item \textsuperscript{43} Id.
\end{itemize}
\end{footnotesize}
however, has several important implications not only for the availability of § 1203 damages, but also for trademark law, copyright law, and for CMI process licensees and licensors.

A. Availability of § 1203 Damages

A broad interpretation of § 1202 would potentially increase the availability of § 1203’s statutory damages. The earlier, narrower § 1202 interpretation made it difficult to prove violation and deterred plaintiffs without cases clearly involving purely digital CMI from attempting to claim § 1203 damages. However, recent courts’ willingness to extend § 1202 applicability may significantly increase the number of statutory damage claims.44 Such claims, if successful, are lucrative. Section 1203 entitles the prevailing party to $2,500 to $25,000 per violation, and the few courts that have interpreted § 1203’s meaning of “violation” have generally counted each individual impression.45 For works distributed online, the total penalty could be astronomical. The threat of such large penalties may cause artists and others creating works under fair use to be more circumspect about the copyrighted works from which they draw inspiration, possibly tilting the litigation balance in favor of copyright holders.46

B. Relationship Between DMCA CMI Requirements and Trademark Law

A § 1202 interpretation broad enough to protect instances of copyright protection and not simply automated protection methods would pose overlapping trademark concerns. In many instances, CMI bears the trademark of the copyright’s owner. A simple example


46 See, e.g., Sony BMG Music Entertainment v. Tenenbaum, No. 07 Civ. 11446-NG (D. Mass. July 9, 2010) (district court nullified a large jury award of statutory damages on due process grounds, even though the award was statutorily valid).
would be the placement of a trademarked business name on a printed photograph. This poses a dilemma; removal of CMI would violate the Act, but retention of CMI in subsequent distribution may violate trademark law.\textsuperscript{47} No court has commented directly on this impasse, though \textit{Associated Press} implied in passing that source citations could not be construed as trademark infringement.

\textbf{C. Effects on Copyright Law}

If § 1202 is applied to all types of CMI, whether analog, digital, manual, or automated, requirements for fair use of copyright information could be significantly altered. At the most textual end of the spectrum, § 1202 makes no exception for fair use; removal or alteration of copyright information is categorically prohibited “without the authority of the copyright owner or law.”\textsuperscript{48} Thus, in its broadest reading, § 1202 practically requires retention of all previous CMI, even for artistic transformations or renditions of existing works, whether digital or analog in content or creation. Such an interpretation would directly oppose the fair use concept that certain types of use do not require the copyright holder’s permission. Any failure to retain this CMI is subject to statutory penalties. A possible defense, however, is to aver that because fair use is fundamentally not infringement, the removal of CMI, whether or not intentional, cannot lead to actual infringement. Thus, one required element of a § 1202 claim would be unfulfilled.

nation of whether the Act protects the CMI in question would require an inquiry into the exact process used to create the CMI as well as the process used to alter it. For example, CMI such as copyright information digitally embedded into an image’s metadata may be protected if a wholly digital process was used in its subsequent transformation under fair use, but not if the work was altered by a manual or analog process (e.g., a physical transformation of a physical print without visible CMI). This approach would emphasize the method by which the CMI was altered or removed, rather than by inquiry into whether CMI was removed at all.

D. Effects on CMI Process Owners

The courts also have not clarified whether CMI conveyance dependent on external process is also protected, and whether those processes must be preserved in subsequent redistribution of the protected work. Only one case, Jacobsen v. Katzer, has commented on the matter. Jacobsen involved two model train hobbyists, both of whom created software frameworks for controlling model train behavior. The plaintiff, who sold the software commercially, filed a multifaceted suit against the defendant, who, under an open-source license, created software that functionally overlapped with the plaintiff’s software. In ruling on the plaintiff’s copyright claims, the Jacobsen court noted in dicta that under §1202, if an automated process is used to imprint CMI in software source code, that process or another like it must retain the original CMI for subsequent impressions. The court also noted that accidental CMI omission might be a violation of § 1202 if the omission takes place via intentional secondary means that unintentionally remove the CMI. For example, if a protected piece of software relies on third-party software both to embed CMI and provide a critical function to the parent software, § 1202 may be violated if that third-party application is replaced with another to enhance the non-CMI function it provides but no longer conveys the attached CMI.

Such an interpretation of the CMI provisions may have significant
implications for CMI-generating process owners, such as software manufacturers. Creators of CMI-generating processes may be forced to give their process, or details about that process, away if a non-original party adapts the work it protects. Both Jacobsen and the statute itself are silent as to whether the owner or licensor of the CMI imprinting mechanism is entitled to compensation if § 1202 mandates its inclusion.

CONCLUSION

Though § 1202 and CMI have historically been a minor component in litigation involving the sweeping Act, some recent court cases have tended to broaden the reach of CMI protection. A broad interpretation of § 1202 will increase the availability of statutory damages, alter copyright balance toward the right’s owners, and affect related trademark law. If courts continue to trend toward broader § 1202 interpretation, they must be prepared to handle a much larger volume of cases posing Act and derivative claims. In addition, litigants must consider several novel effects of CMI doctrine when formulating their copyright complaints or defenses.

PRACTICE POINTERS

- Advise clients to document current CMI conveyance and propagation processes. The clearer the connection between the CMI and the underlying work’s protection scheme is made, the more likely the CMI itself is to be protected.
- Copyright owners should ensure that any copyright information placed on a protected work clearly falls into one of § 1202’s eight defined CMI categories.
- Fully develop copyright-infringement claims before attempting to assert a CMI claim, because the latter is dependent on the former.
- To mitigate legal exposure, advise clients intending to manipulate or integrate copyrighted works under fair use to only remove as much embedded CMI as is necessary. Remind clients that fair use is only a defense and not necessarily a deterrent to litigation.