Chicago-Kent Journal of Intellectual Property

Volume 16 | Issue 1 Article 1

11-22-2016

Open Source Tactics: Bargaining Power for Strategic Litigation

James Skelley

OPEN SOURCE TACTICS: BARGAINING POWER FOR STRATEGIC LITIGATION

JAMES SKELLEY*

* Licensed Attorney, State of California and the District of Columbia. Licensed before the United States Patent Office. The views and analysis in this document are presented merely for purposes of discussion and are not intended as legal advice. Neither are the views and analysis presented herein to be considered the conclusive opinion of the author. Interpretations and conclusions depend greatly upon the particular facts of a given situation and statements by the Author simplified to facilitate understanding should not be construed as the Author's conclusive opinion.

INTRODUCTION

Creative defendants regularly employ tactics compelling plaintiffs to reevaluate or abandon their litigation position. For example, if the defendant discovers that the plaintiff has failed to meet a third-party compliance obligation, the defendant may report, or threaten to report, the failure in order to coerce the plaintiff.[1] Some evidence suggests that hospital management organizations have used this tactic to compel settlements from competitors committing antitrust violations.[2] In some instances, the enforcing third party may be a private, rather than a government, actor.[3] Regardless of the enforcing party's specific character, so long as the violation's disclosure will

1. Though such threats may be susceptible to actions for extortion as discussed in greater detail herein.

2. *See, e.g.*, Nina Youngstrom, *Hospitals Have Options to Level the Playing Field with Noncompliant Competitors*, AISHEALTH (October 26, 2015), https://aishealth.com/archive/rmc102615-01 (reprinted from REPORT ON MEDICARE COMPLIANCE, Volume 24 Issue 38)

> Given the stakes, health care organizations may want to take matters into their own hands, lawyers say . . . We see health care organizations trying very hard and devoting significant resources to compliance efforts, but if their competitors are not following suit, that becomes a real problem . . . there are a number of ways to go about it. They include reporting a competitor's misconduct to its own hotline, using the private right of action under the Racketeer Influenced and Corrupt Organizations (RICO) Act and tipping off the government. . . . The antitrust laws are another avenue for challenging conduct that health care organizations believe is illegal . . . .

Particularly, 18 U.S.C. § 1964(c) permits a civil action for injury following violation of § 1962 regarding racketeering activity. As another example application, consider, *e.g.*, Corcel Corp. v. Ferguson Enterprises, Inc., 551 F. App'x 571 (11th Cir. 2014) wherein a plumber subjected their competition to a RICO suit. *Contrast, e.g.*, Stenehjem v. Sareen 226 Cal. App. 4th 1405 (6th Dist. 2014) (finding extortion). Compare the posture of these cases with subsequent footnotes in this Article regarding the use of a third party beneficiary claim to obviate extortion arguments. While the "influence" diagrams are very similar, the mechanism necessary to pose the threat without implicating extortion may differ greatly.

3. For example, where the compliance breach implicates a contractual obligation for a third party (as is the case with regard to some open source licenses, such as the GPL, which includes a source code copyleft obligation, unlike the MIT and BSD licenses, which do not), the third party may be the enforcing interest. Additionally, the defendant may itself be the enforcing interest in some instances such as in a *qui tam* action (as in the case of certain actions under the False Claims Act). Similarly, though the tactics discussed in this Article refer to open source specifically, much of the same reasoning and logic applies *mutatis mutandis* to third party patent infringement actions.

precipitate action against the plaintiff, the knowledge of the violation may provide the defendant with leverage to effect a favorable settlement.[4]

Open source software presents an emerging and compelling vehicle for these compliance-based defense tactics.[5] It is not entirely clear whether the defendants employed these tactics in the recent *XimpleWare v. Versata* collection of cases (See Section I.A below, hereinafter collectively referred to as *XimpleWare*), but the *XimpleWare* fact pattern illustrates the potential effectiveness and limitations of such tactics. While news and legal commentators have previously discussed *XimpleWare*[6], to the Author's knowledge, *XimpleWare* has not yet received a game-theory analysis thoroughly exploring its rich potential as a compliance-based defensive tactic. Particularly, *XimpleWare* exemplifies an open source topology affording unique strategic opportunities unavailable to many other compliance-based tactics.[7] Accordingly, this Article abstracts from the *XimpleWare* topology to determine when and to what extent a defendant may employ such tactics to enhance their bargaining position (Section II). This Article then examines countermeasures a plaintiff may employ to mitigate such tactics' effectiveness (Section III).

4. Indeed, the threat of enforcement may even suffice to obviate the business dynamic which precipitated the plaintiff's action. For example, consider where a plaintiff sues a defendant to secure market share for their product. The revelation that their product is non-compliant with an upstream agreement, however, coupled with a high cost (perhaps impossible) to remediate, may obviate the plaintiff's ability to remain in the market. In the open source context, this may occur when the plaintiff pervasively integrated a copyleft component into a well-established product offering and the copyleft requirements prevent profitable licensing terms.

5. In addition to the benefits relative to extortion discussed herein, copyright infringement also proceeds under the "separate-accrual" rule, wherein the three-year statute of limitations is reset for each new infringing act. *See, e.g.*, Petrella v. MGM, 134 S. Ct. 1962, 1964 (2014) ("A claim ordinarily accrues when an infringing act occurs. Under the separate-accrual rule that attends the copyright statute of limitations, when a defendant has committed successive violations, each infringing act starts a new limitations period. However, under § 507(b), each infringement is actionable only within three years of its occurrence.").

6. *See, e.g.*, Jaideep Reddy, *The Consequences of Violating Open Source Licenses*, BERKLEY TECH. L.J,: THE BOLT (November 8, 2015), http://btlj.org/2015/11/consequences-violating-open-source-licenses/ (While recognizing that open source breaches may be costly, commentators generally stop short of rigorously characterizing that cost or exploring the factors affecting its viability as a negotiation tool).

7. In many ways, open source software presents a strategic "perfect storm" for the threat-maker. As discussed herein, open source asymmetrically benefits the threat-maker in that it obviates extortion counterarguments, permits open information gathering by the threat-maker (many companies' software can be reverse-engineered or publicly reviewed), provides for "separate accrual" of copyright infringement actions, and favors the threat-maker in the timing with which they threaten the infringer, or approach the copyright-holder for purchase. Such asymmetries will likely increase the tactic's prevalence in the future.

I. EXAMPLE PATTERN: XIMPLEWARE V. VERSATA

A. XimpleWare Specific Litigation Topology

XimpleWare, as used in this Article, refers to the following five cases, three in Texas and two in California:

1. **Texas Federal, Western District**: Case No. 1:10cv792 - *Versata Software Inc. v. Infosys*;
2. **Texas State, Travis County**: Case No. D-1-GN-12-003588: - *Versata Software Inc. f/k/a Trilogy Software, Inc. and Versata Development Group Inc. f/k/a Trilogy Development Group Inc. v. Ameriprise Financial Inc., et al.;*
3. **Texas Federal, Western District**: Case No. 1:14-cv-12 - *Versata Software Inc. v. Ameriprise Financial Services Inc. et al.*;
4. **California Federal, Northern District**: Case No. 3:13cv5160: - *XimpleWare Corp. v. Versata Software Inc., Trilogy Development Group, Inc., Ameriprise Financial, Inc., Ameriprise Financial Services, Inc., Aurea Software, Inc.*; and
5. **California Federal, Northern District**: Case No. 5:13cv5161 - *XimpleWare Corp. v. Versata Software Inc., Aurea Software Inc., Trilogy Development Group, Inc., Ameriprise Financial Services, Inc., Ameriprise Financial, Inc., United HealthCare Services, Inc., Waddell & Reed, Inc., Aviva USA Corporation, Metropolitan Life Insurance Company, Pacific Life Insurance Company, The Prudential Insurance Company of America, Inc., Wellmark, Inc.*

Initially, in the Texas cases, Versata accused Ameriprise and its affiliate Infosys of violating the technology license agreement for Versata's Distribution Channel Management ("DCM") software.[8] Particularly, Versata alleged that Infosys decompiled and reverse engineered the DCM's source code in 2008-2009, violating several express prohibitions in the DCM agreement (Action #1).[9] Versata alleged that Infosys then used the knowledge gained from the decompilation on behalf of Ameriprise (Actions

8. *See, e.g.,* Pl's. Third Am. Compl. at 4, Versata Software Inc. v. Infosys Technologies Ltd. (2014), (No.1:10-cv-00792-SS), 2014 WL 10321037.

> Infosys, acting through its agents and employees, improperly accessed, utilized, copied, disassembled, and decompiled Versata's confidential source code in 2008 and 2009. In 2008, Infosys was providing software maintenance services for Ameriprise at the same time that Versata provided software services to Ameriprise. Infosys' agents and employees, working on Versata's code base at Ameriprise, decompiled Versata's DCM source code and created new code for the benefit of Infosys.

9. *Id.* at 4; 9-11, "Subsections (d) and (e) are even more specific, and prohibit Infosys from copying, reproducing, disassembling, decompiling, or reverse engineering Versata's confidential information".

#2, #3).[10] Consequently, Versata alleged copyright infringement, misappropriation of trade secrets, and unfair competition, among other causes of action.[11]

During the course of this Texas litigation, however, Ameriprise discovered that Versata's DCM itself did not appear to comply with the license terms for at least one of its upstream components.[12] Particularly, DCM used a software component called VTD-XML, which was developed by the California company XimpleWare. XimpleWare released VTD-XML under the General Public License v2.0 (GPLv2.0), an open source license.[13] The GPLv2.0 requires, among other things, that downstream distributors of derivative works provide the distribution under the GPLv2.0, and that the distributor make available the derivative work's source code to downstream recipients.[14] According to court documents, upon discovering that Versata's distribution of DCM did not comply with the GPL's requirements, Ameriprise notified XimpleWare of the noncompliance.[15]

XimpleWare subsequently initiated litigation against both Versata and Ameriprise in California (Actions #4 and #5) based upon the noncompliant distribution and use of the GPLv2.0 licensed VTD-XML (Ameriprise, as a non-compliant downstream user of the code was likewise alleged to have committed copyright infringement).[16] XimpleWare also sued Versata's customers (e.g., Pacific Life Insurance, Wellmark, Inc., etc.) for various actions, including, e.g., patent infringement.[17] While courts have not yet considered all provisions of the GPLv2.0 specifically, courts have generally

10. *Id.* at 10, "Infosys employees used and copied the decompiled code on numerous occasions, for commercial gain, in their work for Ameriprise".

11. *Id.*

12. *See, e.g.*, Y. Peter Kang, *XimpleWare, Versata Settle Insurance Software IP Dispute*, LAW360, (Februrary 11, 2015, 6:24 PM EST), http://www.law360.com/articles/620898/ximpleware-versata-*settle-insurance-software-ip-dispute.*

13. *VTD-XML: The Future of XML Processing*, SOURCEFORGE, http://vtd-xml.sourceforge.net/.

14. *See, e.g.*, *GNU General Public License , version 2*, GNU Operating System (June 1991), http://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html.

> 3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
>
> a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> . . .
>
> This General Public License does not permit incorporating your program into proprietary programs.

15. Complaint at 9, Ximpleware, Inc., v. Versata Software, Inc., et al., No. 3:13-cv-05160-SI (N.D. Cal. Nov. 5, 2013) ("During the prosecution of that lawsuit, Ameriprise informed XimpleWare that it had discovered portions of XimpleWare's GPL-licensed Source Code in the source code of Versata's DCM product").

16. *Id.* at 10-11.

17. Complaint at 9-14, Ximpleware, Inc., v. Versata Software, Inc., et al., No. 5:13-cv-05161-PSG (N.D. Cal. Nov. 5, 2013).

expressed a willingness to enforce open source licenses.[18] For example, the Court of Appeals for the Federal Circuit enforced the Artistic License in *Jacobsen v. Katzer*.[19] In face of all these actions, each of the *XimpleWare* parties eventually settled their respective litigations.[20]

Figure 1 summarizes the *XimpleWare* litigation topology in graphical form.

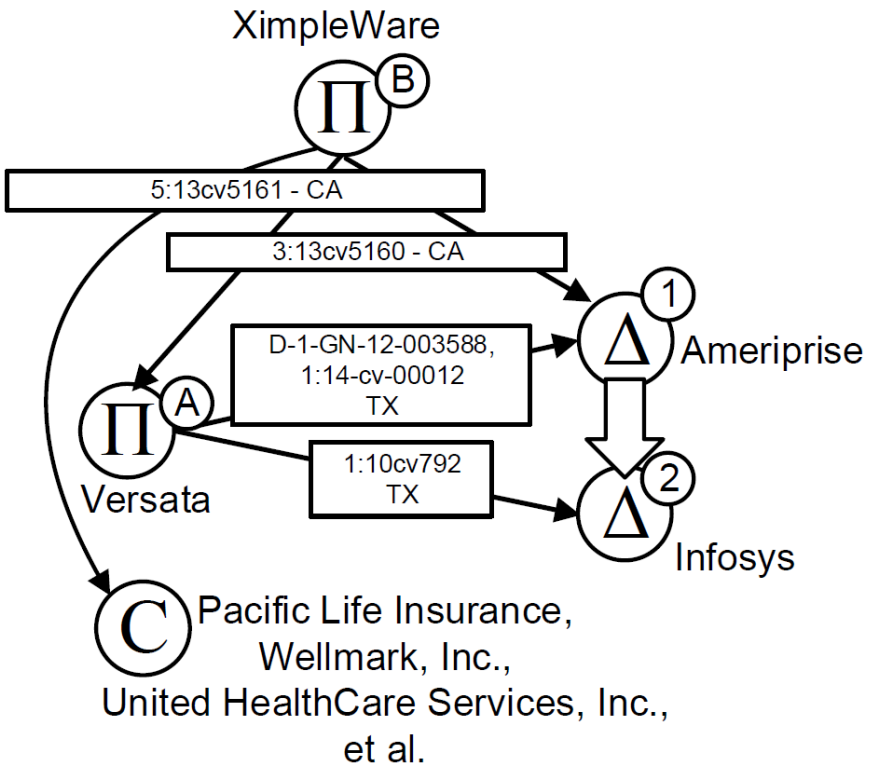

FIGURE 1: Simplified *XimpleWare* Litigation Topology

18. *Id.*

19. *See, e.g.*, Jacobsen v. Katzer and Kamind Associates, Inc., 535 F.3d 1373, 1381 (Fed. Cir. 2008) ("Copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material."). Note, however, that CAFC considered the Artistic License, rather than the GPL, in *Katzer*. While at least some of the GPL's provisions are likely enforceable, some, such as the copyleft implications for dynamic linking, remain quite controversial.

20. *See, e.g.*, Peter Kang, *XimpleWare, Versata Settle Insurance Software IP Dispute*, Law360 (Feb. 11, 2015, 6:24 PM), http://www.law360.com/articles/620898/XimpleWare-versata-settle-insurance-software-ip-dispute.

What can a practitioner discern from this pattern? Was it prudent for Ameriprise to inform XimpleWare of Versata's breach? Did Ameriprise's disclosure to XimpleWare improve Ameriprise's bargaining position? What could Versata have done differently to mitigate such behavior? This Article provides an analytical framework for considering and answering, or at least clarifying, these questions.

B. Generalized Litigation Topology

Figure 2 abstracts from the *XimpleWare* fact pattern provided above to illustrate a more generalized set of relationships.

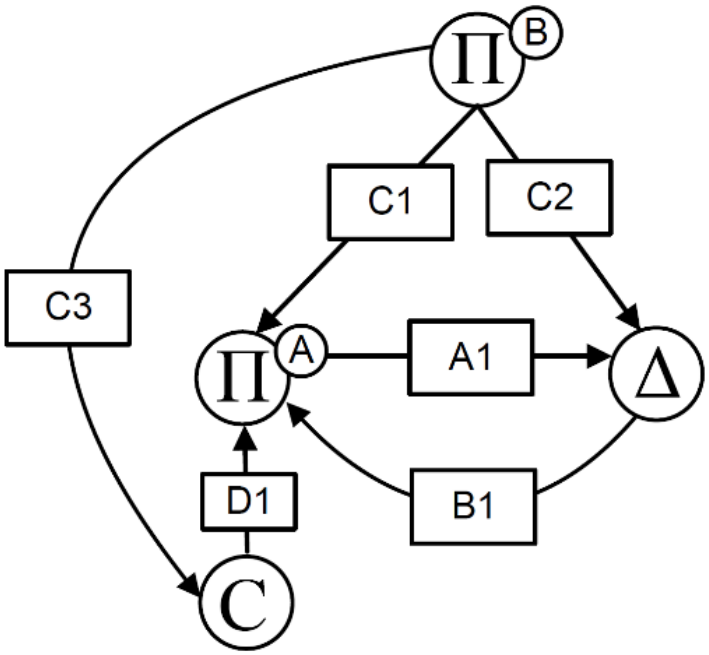

FIGURE 2: Generalized Strategic Litigation "Spatial" Topology

In this diagram, the arrows represent "influence" pressures, which may take the form of litigation, but may also represent more general methods of coercion (e.g., they may include "market pressures" as when customers elect a substitute product). The reader may find it useful to print this diagram and keep it at hand for the remainder of the discussion. The symbols are as follows:

Parties

Π^A: The "plaintiff" party(ies) (e.g., Versata) bringing the initial action, or having cause for action, **A1** against the "defendant" party(ies) **Δ**;

Δ: The "defendant" party(ies) (e.g., Ameriprise) to **Π^A**'s action;

Π^B: The true copyright owner (e.g., XimpleWare) of the open source software distributed in a non-compliant fashion by **Π^A**; and

C: The "customers" of **Π^A** who use **Π^A**'s non-compliant software (as in *XimpleWare* **Δ** may also be a member of **C**).

Influence Pressures (e.g., Actions / Causes for Action)

A1: The initial action, or basis for action, by **Π^A** against **Δ**;

B1: **Δ**'s action, which may be directly responsive to **A1**, e.g., a counterclaim, brought against **Π^A**;

C1, C2: The copyright owner **Π^B**'s action, or basis for action, against **Π^A** and **Δ** respectively (note that in many fact pattern variations **C2** will not exist);

C3: The copyright owner **Π^B**'s action, or basis for action, against the downstream customers **C** of **Π^A**; and

D1: The responsive action, or pressured response, by the downstream customers **C** against **Π^A**.

Note that not all of the influence pressures may be present at the same time (initially, e.g., there may only be **A1**).

Section II analyzes this topology to discern general principles governing **Δ**'s behavior when threatening **Π^A** with disclosure of **Π^A**'s open source violation. Section III then briefly considers countermeasures to these principles available to **Π^A**.

II. COMPLIANCE-BASED DEFENSE TACTICS

This Section focuses upon **Δ**'s perspective, specifically, how **Δ** may mitigate or otherwise influence **A1** in view of the pressures upon **Π^A** following disclosure. Particularly, unlike other compliance-based tactics, e.g., situations where **Δ** has not itself directly suffered harm, **Δ** may often threaten **Π^A** without fearing allegations of extortion. **Δ** will often be a third party-beneficiary of the open source license and most jurisdictions will not consider the threat of a legitimate third-party claim (and in some cases, even

a questionable claim) an extortive act.[21] As discussed in greater detail below, such claims will have the incidental effect of informing **Π^B^** of the noncompliance and therefore, are often coeval with threatening such notification. This freedom permits **Δ** greater latitude when structuring its threat as compared to other compliance-based tactics susceptible to extortion counter actions.[22]

Thus, let us assume that **Δ** is rational, i.e., that **Δ** is not merely seeking to punitively harm **Π^A^** by disclosing the violation without consideration to the consequences.[23] Rather, **Δ** seeks to make a credible threat to **Π^A^** regarding the disclosure, likely to precipitate a favorable conclusion of **A1** for **Δ**. **Π^A^** will only consider such a threat credible and take action regarding **A1** if: 1) the resultant harm to **Π^A^** from the disclosure will meaningfully compel **Π^A^**

21. In *XimpleWare* specifically, the defendant Ameriprise sought to compel Versata to disclose its source code in compliance with the GPL as a third party beneficiary. Though the court did not ultimately rule on the motion, a favorable ruling would have been likely in view of the other case law identified herein. *See, e.g.*, Remand Order at 9, Versata Software, Inc., v. Ameriprise Financial, Inc. (2014) (No.A-1-14-cv-12-ss), 2014 2014 WL 950065 ("Having found no basis for federal jurisdiction over this claim, the Court need not determine whether Ameriprise has standing to enforce the GPL as a third-party beneficiary."); *See also* GPL_response, Versata Software, Inc., v. Ameriprise Financial, Inc. (2014) (No.A-1-14-cv-12-ss), 2014 WL 950065 ("Ameriprise asserts that it is a third-party beneficiary of the GNU General Public License (Doc. No. 9-3, the 'GPL') and as such is entitled to receive the source code to Versata's software product called, Distribution Channel Management ('DCM'). Pursuant to the GPL, any party who, like Versata, distributes software that incorporates code licensed under the GPL must provide all the source code for the software being distributed, including formerly proprietary code. Ameriprise seeks to enforce the contractual right requiring Versata to produce its DCM source code to Ameriprise. Versata incorrectly asserts that copyright law preempts Ameriprise's claim to the source code. Ameriprise's claim to be a third-party beneficiary of the GPL, however, is not preempted because the rights granted by the GPL are essentially the opposite of copyright and, in particular, there is no equivalent third-party-beneficiary claim in copyright law").

22. Note that this third party beneficiary basis may serve to obviate claims of extortion by **Π^A^** as **Δ** is merely "exercising its rights". Generally, a threat to file a lawsuit, even if made in bad faith, does not constitute extortion. As noted by Justice Holmes, "'As a general rule, even if subject to some exceptions, what you may do in a certain event you may threaten to do, that is, give warning of your intention to do in that event, and thus allow the other person the chance of avoiding the consequences.'" McKay v. Retail Auto. Salesmen's Local Union No. 1067, 16 Cal. 2d 311, 321 (1940) (quoting Vegelahn v. Guntner, 167 Mass. 92, 107 (1896)), cert. denied, 313 U.S. 566 (1941); *See also, e.g.*, U.S. v. Pendergraft, 297 F.3d 1198, 1204 (11th Cir. 2002) ("A threat to litigate, by itself, is not necessarily "wrongful" within the meaning of the Hobbs Act. After all, under our system, parties are encouraged to resort to courts for the redress of wrongs and the enforcement of rights.");

Accordingly, while for simplicity, this Article often characterizes **Δ**'s threat to **Π^A^** as "I'll tell **Π^B^**", in practice, the threat would more typically resemble "I'll file my third party beneficiary counterclaim indirectly notifying **Π^B^**". The latter may be especially likely in jurisdictions, such as California, affording **Π^A^** a civil cause of action for extortion.

23. Some practitioners have scoffed to the Author at this level of analysis, responding (to paraphrase) "isn't it enough just to have one more vehicle for hurting the other fellow?" Such a crude assessment ignores the possibility that disclosure may irrevocably escalate the situation, forcing a state of total-war between otherwise reconcilable parties. Still, in some situations, practitioners may be inclined to disclose without threatening to avoid allegations of extortion. Distinguishing extortion from settlement bargaining may depend upon the third party beneficiary options under **B1**, the manner in which **Δ** makes **Π^A^** aware of the noncompliance, the relationship between the violation an **A1**, and case law in the relevant jurisdiction. As previously discussed, most courts would likely favor the third party beneficiary claim.

to resolve **A1**; and 2) the harm to **Δ** resulting from the disclosure does not itself obviate **Δ**'s reasons for disclosing.[24] These requirements are referred to as the "credibility conditions" herein and are discussed in greater detail in Section II.A.[25]

With an eye to these credibility conditions, **Δ** will consider: 1) is it worthwhile for **Δ** to even pose the threat (Section II.B); and if so, 2) how should **Δ** pose the threat to $\mathbf{\Pi^A}$ so that the threat is most effective (Section II.C)? Phrased differently, **Δ**, as a rational actor, will reason backward from $\mathbf{\Pi^A}$'s perceived consequences of the disclosure to determine if it is worth threatening to disclose (Section II.B). If it is worth threatening to disclose, **Δ** should present the threat to $\mathbf{\Pi^A}$ so as to maximize **Δ**'s bargaining gains (Section II.C).

A. Qualitative Assessment of the Threat Credibility Conditions

To reiterate, for **Δ**'s disclosure threat to $\mathbf{\Pi^A}$ to be effective, $\mathbf{\Pi^A}$ must believe two things:

Condition 1: Disclosure will substantially mitigate $\mathbf{\Pi^A}$'s willingness to pursue **A1**; and
Condition 2: Disclosure will not unreasonably expose **Δ** to risk.

Let us restate these conditions more rigorously in terms of pseudo-algebraic parameters. These parameters will allow us to more succinctly categorize the effects of each party's actions.[26] Just as we've assumed that **Δ**

24. *See, e.g.*, THOMAS C. SCHELLING, ARMS AND INFLUENCE, Introduction Pg. 3 ("But in the world of coercive diplomacy, threats and assurances must be balanced through a process **of clear and credible signaling**, and enforceable bargains must be struck short of total defeat or victory for either side. **Without credible threats, coercion is obviously ineffective**. But what is less well understood is that coercion is also unlikely to be effective without **simultaneously transmitted credible assurances that the threat is fully conditional** upon the target's behavior and that the target's key security interests will not be harmed if it complies with the demands of those leveling the threats. **Without receiving both threats and assurances in concert, the target of a coercive threat has little incentive to comply with the demands being made**," emphasis added).

25. Indeed, that the conditions are in fact true, and not simply perceived as true, may be more effective. Thomas Schelling, *An Essay on Bargaining*, 46 AM. ECON. REV. 281, 281-306 (1956) ("How does one person make another believe something? The answer depends importantly on the factual question, 'Is it true?' It is easier to prove the truth of something that is true than of something false.").

26. When performing analysis such as these, the author rarely adheres to a "strict" application of game theory. Indeed, some researchers question if it if even possible to apply game theory in practical contexts. *See, e.g.*, Ariel D. Procaccia, *Game Theory Is Useful, Except When It Is Not*, SYMPOSIUM MAGAZINE (Dec. 31, 2013) http://www.symposium-magazine.com/game-theory-is-useful-except-when-it-is-not-ariel-d-procaccia/. The Author often references the "Surprise Hanging Paradox" as an example of an over-confident application of induction-style game theory arguments. *See, Unexpected hanging paradox*, WIKIPEDIA, https://en.wikipedia.org/wiki/Unexpected_hanging_paradox (last visited Nov. 15, 2016); *See also, e.g., How Common Sense May Trump Game Theory*

is rational, let us assume that $\mathbf{\Pi^A}$ is rational (we will relax these assumptions as we proceed).

Regarding the first condition, assume that $\mathbf{\Pi^A}$ has initiated or threatened **A1** because $\mathbf{\Pi^A}$'s perceived *benefit* to initiating **A1** ($Benefit_{A1}$) exceeds $\mathbf{\Pi^A}$'s perceived *cost* for initiating **A1** ($Cost_{A1}$), i.e.:

$$Benefit_{A1} > Cost_{A1} \quad (1)$$

For example, $\mathbf{\Pi^A}$ may be willing to pay $2 Million in attorney fees ($Cost_{A1}$) for a $40 Million judgment ($Benefit_{A1}$). Absent action by **Δ**, this cost may simply be $\mathbf{\Pi^A}$'s litigation expenses. If $\mathbf{\Pi^A}$ believes that it will recover attorney fees, these expenses may be perceived as nominal or zero. To make $\mathbf{\Pi^A}$'s pursuit of **A1** untenable, or at least very unpalatable, **Δ** should seek to increase *the additional cost to* $\boldsymbol{\Pi^A}$ *from the open source violation disclosure* ($Disclosure\_Cost_{\Pi A}$) so as to negate $Benefit_{A1}$. Preferably, $\mathbf{\Pi^A}$ should believe at the time **Δ** poses the threat that:

$$Benefit_{A1} < Cost_{A1} + Disclosure\_Cost_{\Pi A} \quad (2)$$

If Equation (2) is true, then the threat to disclose to $\mathbf{\Pi^A}$ would credibly obviate the benefit of **A1**. Accordingly, $\mathbf{\Pi^A}$ would be unreasonable to ignore the threat. If Equation (2) is not true, then $\mathbf{\Pi^A}$ should be indifferent to **Δ**'s threat.

Setting aside the first condition, for now, the second credibility condition requires that **Δ** not unreasonably expose itself to risk by making the disclosure. Particularly, as evidenced by **C2**, the disclosure may likewise result in **Δ** becoming subject to suit by $\mathbf{\Pi^B}$. In addition, **Δ** may become exposed to procedural costs/risks if it discloses, e.g., where a protective order or nondisclosure agreement is in place prohibiting such disclosures (See, Section II.C.2 *infra*). These *costs to* $\boldsymbol{\Delta}$ *resulting from the disclosure* are cumulatively referred to herein as $Disclosure\_Cost_{\Delta}$.[27] If $Disclosure\_Cost_{\Delta}$ is much greater than the loss **Δ** would suffer if $\mathbf{\Pi^A}$ succeeds in **A1** ($A1\_Loss_{\Delta}$), then it is not credible that **Δ** would disclose and incur the

https://blogs.cornell.edu/info2040/2014/09/28/how-common-sense-may-trump-game-theory/ (last visited Oct. 30, 2016). Accordingly, the author instead finds it useful to use quantitative relations only insofar as they inform more qualitative assessments, hence, "pseudo-algebraic" reasoning.

27. To simplify, let us incorporate the probability of these costs being incurred into their qualitative value (e.g., discounting based upon their likelihood and **Δ**'s risk aversion, etc.). A practitioner presented with very specific facts may instead consider the variance associated with each parameter's probability in their analysis.

additional *Disclosure_Cost*$_{\Delta}$.[28] Stated differently, if **A1** only presents a *de minimis* harm to **Δ**, but disclosure presents a *very great* harm, why would **Δ** put itself in jeopardy of such a greater harm to avoid a smaller harm?[29] Thus, the second credibility condition appears to imply that $\mathbf{\Pi^A}$ believe:

$$A1\_Loss_{\mathbf{\Delta}} \gg Disclosure\_Cost_{\mathbf{\Delta}} \quad (3)$$

However, this statement only captures a subset of the circumstances under which the second condition would be credible. As mentioned, $\mathbf{\Pi^A}$ will expect **Δ** to suffer both *A1_Loss*$_{\Delta}$ and *Disclosure_Cost*$_{\Delta}$ following disclosure.[30] Accordingly, a more accurate statement of the second condition would reflect $\mathbf{\Pi^A}$'s belief that **Δ** is willing to bear both *A1_Loss*$_{\Delta}$ and *Disclosure_Cost*$_{\Delta}$ following disclosure. This "willingness" is contextual. For example, if *A1_Loss*$_{\Delta}$ will clearly bankrupt **Δ** then what reason has **Δ** to fear *Disclosure_Cost*$_{\Delta}$? The second condition becomes irrelevant – **Δ** has nothing to lose and only something to gain by disclosing. Similar contextual variations will scale terms in the inequality. To account for this contextual effect, let us introduce a proportional weighting factor $C_{context}$ adjusting *Disclosure_Cost*$_{\Delta}$ to account for $\mathbf{\Pi^A}$'s belief in **Δ**'s appreciation of future losses resulting from the disclosure.

$$A1\_Loss_{\mathbf{\Delta}} > C_{context} * Disclosure\_Cost_{\mathbf{\Delta}} \quad (4)$$

Thus, in the bankruptcy scenario discussed above, $C_{context}$ will be 0, as **Δ** will consider the additional *Disclosure_Cost*$_{\Delta}$ irrelevant. Similarly, if *Disclosure_Cost*$_{\Delta}$ presents a finite, manageable harm, $C_{context}$ becomes 1. If $\mathbf{\Pi^A}$ relaxes **Δ**'s rationality (e.g., as the parties approach an irrational state of total conflict) $C_{context}$ can become < 1, etc.

Note that $C_{context}$ has a (roughly) inverse effect upon the first condition. When $C_{context}$ is 0, as in the bankruptcy scenario, **Δ** may as well enter a state

28. Note that *A1_Loss*$_{\Delta}$ includes both the effects of judgment against **Δ** as well as **Δ**'s cost to defend. This asymmetry relative to *Cost*$_{A1}$ will become relevant in the subsequent discussion of bargaining power. To restate the matter more explicitly, increasing *Cost*$_{A1}$ (e.g., increasing $\mathbf{\Pi^A}$'s attorneys' fees) lowers the stakes for $\mathbf{\Pi^A}$, but increasing *A1_Loss*$_{\Delta}$ (e.g., increasing **Δ**'s attorneys' fees) increases the stakes for **Δ**.

29. In other words, the response would be disproportionate. Typically, Menelaus' waging massive inter-state warfare is a disproportionate response to the isolated act of Helen's infidelity. Of course, these things happen, they're just not rational. $C_{context}$ will be used to relax rationality in the subsequent sections.

30. To rephrase the observation, $\mathbf{\Pi^A}$ will generally believe the threat if **Δ**'s end condition is plausible. Not only a small *Disclosure_Cost*$_{\Delta}$ but any *Disclosure_Cost*$_{\Delta}$ meeting that condition will suffice.

of total conflict (i.e., the motive is no longer to influence $\mathbf{\Pi^A}$, but simply to cause harm). Accordingly, let us state the final, pseudo-algebraic parameter representations of the credibility conditions as follows:

$$\textbf{\textit{Condition 1}}: Benefit_{\boldsymbol{A1}} < \frac{(Cost_{\boldsymbol{A1}} + Disclosure\_Cost_{\boldsymbol{\Pi A}})}{C_{context}} \quad (5)$$

$$\textbf{\textit{Condition 2}}: A1\_Loss_{\boldsymbol{\Delta}} > C_{context} * Disclosure\_Cost_{\boldsymbol{\Delta}} \quad (6)$$

As mentioned in the preceding footnote, this framework is clearly not intended to establish "hard and absolute" numerical rules and relationships. The amorphous character of $C_{context}$ will require the practitioner to carefully consider their particular situation before attempting to assign a numerical value.[31] Indeed, the value of $C_{context}$ in Condition 1 may not be exactly the same in Condition 2, and separate parameters may be more suitable. For this Article's purposes, however, this framework will permit us to more rigorously evaluate the consequence to **Δ**'s threat from each of the legal considerations.

Thus, Conditions 1 and 2 inform **Δ**'s decision to disclose and the threat's persuasive effect upon $\mathbf{\Pi^A}$. Section II.B focuses on Condition 1, discussing how **Δ** can maximize $Disclosure\_Cost_{\boldsymbol{\Pi A}}$ and minimize $C_{context}$ so as to persuade $\mathbf{\Pi^A}$ that disclosure will cause $\mathbf{\Pi^A}$ genuine harm (in other words, "is posing the threat worthwhile to **Δ**?"). Section II.C then focuses on both Conditions 1 and 2, discussing how **Δ** can minimize $Disclosure\_Cost_{\boldsymbol{\Delta}}$ and again minimize $C_{context}$ by posing the threat in a credible manner (in other words, "how should **Δ** pose the threat?"). As discussed in Section II.C, some of these actions (e.g., purchasing $\mathbf{\Pi^B}$'s copyright) may have the secondary effect of also increasing $Disclosure\_Cost_{\boldsymbol{\Pi A}}$.

*B. Influencing **A1** - "Is Threatening Worthwhile"?*

With regard to Condition 1, **Δ** should maximize $Disclosure\_Cost_{\boldsymbol{\Pi A}}$ and minimize $C_{context}$. $Disclosure\_Cost_{\boldsymbol{\Pi A}}$ generally depends upon three consequences following from the disclosure:

1) The remedies sought by $\mathbf{\Pi^B}$ against $\mathbf{\Pi^A}$;

31. Consider, e.g., a somewhat particular situation where **Δ**'s board of directors anticipate declaring bankruptcy and pursuing a new venture dependent upon the goodwill of $\mathbf{\Pi^A}$. Thus, the preceding motivations following from bankruptcy no longer apply here and $C_{context}$ is no longer 0. The parameter's new value will depend upon how much the disclosure jeopardizes the future venture, a likely qualitative, amorphous consideration. In application, the practitioner will need to consider their specific circumstances.

2) Newly available counterclaims **B1** by **Δ** against **Π^{A}**; and
3) Pressures **D1** from downstream customers **C** precipitated by **C3**.

The following sections consider these consequences in turn.

1. The Remedies Sought by **Π^{B}** Against **Π^{A}**

An open source license's breach may precipitate several causes of action in **C1**. In past cases, direct copyright infringement, indirect copyright infringement, violation of the Lanham Act § 43, unfair competition, breach of contract, tortious interference with business relations / intentional interference with prospective economic advantage, misappropriation, breach of implied covenant of Good Faith and Fair dealing, unjust enrichment, etc. have all appeared.[32] Naturally, plaintiffs typically seek both injunctive and monetary relief for these causes of action where available.[33] It is important that **Δ** carefully consider the character of the injunctive and monetary relief sought by **Π^{B}** as these will inform value of *Disclosure_Cost$_{\Pi A}$*. Additionally, this relief will also influence the likelihood that **Π^{B}** will bring the action **C1** in the first place (indeed the foundation for **Δ**'s threat to **Π^{A}**). To simplify, let us assume that this probability is already reflected within *Disclosure_Cost$_{\Pi A}$*, since they are (to a certain extent) positively correlated (i.e., the more value **Π^{B}** ascribes to the action **C1**, the more likely **Π^{B}** is to bring the action **C1**). Thus, the greater the consequences to **Π^{A}** from **Π^{B}**'s injunctive and monetary relief, the higher *Disclosure_Cost$_{\Pi A}$*.

a. Injunctive Relief

In most open source breach scenarios, the preferred relief is injunctive. In *Jacobsen v. Katzer*, for example, the Court of Appeals for the Federal Circuit upheld a request for preliminary injunction where the defendant had not complied with the terms of the Artistic License.[34] The court observed that in many cases, monetary damages would not be available to an open source plaintiff as there were no lost profits associated with the breach:

> Copyright licenses are designed to support the right to exclude; money damages alone do not support or enforce that right. **The choice to exact consideration in the form of compliance with the open source requirements of disclosure and explanation of changes, rather than as a dollar denominated fee, is entitled to no less legal recognition. Indeed, because a calculation of damages is inherently speculative, these types of license**

32. *E.g.*, Complaint at 1, Ximpleware, Inc., v. Versata Software, Inc., et al., No. 3:13-cv-05160-SI (N.D. Cal. Nov. 5, 2013) (this particular list is taken in part from the XimpleWare complaint).
33. *Id.*
34. *Jacobsen*, 535 F.3d at 1376.

> **restrictions might well be rendered meaningless absent the ability to enforce through injunctive relief**.[35]

For a permissive license, e.g., the MIT or BSD license, simply including an absent copyright notice may suffice to cure the deficiency. Consequently, the injunctive relief for these licenses typically present poor vehicles for increasing $Disclosure\_Cost_{\Pi A}$, as compliance may simply be a tedious inconvenience for $\mathbf{\Pi^A}$ and **C**. While not substantial, such smaller compliance costs may still serve **Δ**'s purposes if $Benefit_{A1}$ is "low" or $Cost_{A1}$ is "high". Indeed, in *Jacobsen v. Katzer*, the defendant incurred both the costs of a district court and federal appeal by simply failing to include the required notice.[36] Such small stakes litigation will likely be the exception, rather than the rule, however, given the high costs involved in $\mathbf{\Pi^A}$'s bringing legal action.

In higher stakes litigation, **Δ** would need a more compelling violation if **Δ** intends to rely upon the injunction to increase $Disclosure\_Cost_{\Pi A}$. Less permissive open source licenses in conjunction with $\mathbf{\Pi^A}$'s business structure, may serve this purpose. For example, some open source licenses include strong copyleft requirements (e.g., the GPL or Sleepycat licenses). These copyleft provisions may require not only that the original open source code be made available in source code form, but that $\mathbf{\Pi^A}$ provide its entire commercial product (or a substantial portion) in source code form.[37] Whether this is the case will depend upon the exact terms of the license and the nature of $\mathbf{\Pi^A}$'s commercial product.[38] Requiring that $\mathbf{\Pi^A}$ disclose its source code

35. *Id.* at 1382 (emphasis added).

36. *Id.*

37. For example, the GPL has always been viewed as applying to both statically and dynamically linked libraries, *See Frequently Asked Questions about the GNU Licenses*, GNU OPERATING SYSTEM (May 26, 2016) http://www.gnu.org/licenses/gpl-faq.en.html#GPLStaticVsDynamic (05/26/2016) ("Does the GPL have different requirements for statically vs dynamically linked modules with a covered work? (#GPLStaticVsDynamic) No. Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, the terms and conditions of the GNU General Public License cover the whole combination.). *See also* GNU GENERAL PUBLIC LICENSE, version 2, License, http://www.gnu.org/licenses/gpl-faq.en.html# (05/26/2016) (What legal issues come up if I use GPL-incompatible libraries with GPL software?"). The consequences of a violation in this context will need to be carefully evaluated by **Δ**. If the linking is to an isolated module of $\mathbf{\Pi^A}$'s product, then only that module will be subject to the GPL.

38. To maximize $Disclosure\_Cost_{\Pi A}$ the open source code would ideally be interwoven with the commercial product such that the license's terms apply to the product's entirety and such that the open source code cannot be easily separated or substituted. When this is not the case, however, the violation may still suffice to raise $Disclosure\_Cost_{\Pi A}$ so long as $\mathbf{\Pi^B}$ has a basis for demonstrating sufficient damages. Consider a violation of the GPLv2.0. In some ways, whether the code was dynamically linked, statically linked, or copied directly is irrelevant. This is because when $\mathbf{\Pi^B}$ experiences grave financial harm from the violation, that harm is unlikely to arise from the infringement itself (since compliant distributions were freely available). Rather, $\mathbf{\Pi^B}$'s financial interest arises from secondary factors, such as the market or $\mathbf{\Pi^B}$'s business structure. But if this the character of the harm, then another basis (e.g., an unfair competition claim) probably suffices to $Disclosure\_Cost_{\Pi A}$.

may have devastating consequences for $\mathbf{\Pi^A}$. For example, where $\mathbf{\Pi^A}$ operates in the defense industry or in a litigious patent market, source code availability may fail to comply with the DFARs or expose $\mathbf{\Pi^A}$ to an infringement action, respectively.[39] Perhaps more importantly, copyleft provisions may also deny the addition of commercial terms.[40] These commercial terms may have been required to make $\mathbf{\Pi^A}$'s product profitable. Much service software includes nontrivial royalty determinations based upon the character of the customer's usage.[41] Requiring these terms' removal could be devastating to $\mathbf{\Pi^A}$.

Thus, an injunction requiring compliance with a copyleft license may deny $\mathbf{\Pi^A}$ the enjoyment of a market advantage it previously held relative to its competitors. $Disclosure\_Cost_{\Pi A}$ will then include at least: 1) the future loss of this advantage; 2) the remediation cost for the past violations; and 3) reputational harm from those who would have benefited from the earlier compliance. Indeed, if financial data regarding $\mathbf{\Pi^A}$'s past profits are available, $\mathbf{\Delta}$ would likely seek to ascertain the loss in market advantage to clarify $Disclosure\_Cost_{\Pi A}$. Similarly, $\mathbf{\Delta}$ should be able to readily ascertain the consequences to existing market share when remediating (discussed in greater detail below with respect to **C3** and **D1**).

Despite these potentially onerous outcomes, there may be factors insulating $\mathbf{\Pi^A}$ from monetary damage flowing from the injunction. Obviously, insurance can provide such insulation, but *prolonged noncompliance itself* may also serve to insulate $\mathbf{\Pi^A}$ from these injunctive damages. Particularly, being the "first to market" is often the dispositive factor in software sales as the first entrant may displace opportunities for follow-on entrants.[42] $\mathbf{\Pi^A}$ may have eliminated the competition in this manner

39. *See GNU General Public License, version 2*, GNU OPERATING SYSTEM (June, 1991), http://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html ("(b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License"). *See, e.g. Clarifying Guidance Regarding Open Source Software (OSS)*, DEPARTMENT OF DEFENSE (Oct. 16, 2009), http://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/2009OSS.pdf ("The use of any software without appropriate maintenance and support presents an information assurance risk. Before approving the use of software (including OSS), system/program managers, and ultimately Designated Approving Authorities (DAAs), must ensure that the plan for software support (e.g., commercial or Government program office support) is adequate for mission need.").

40. *See GNU General Public License, version 2*, GNU OPERATING SYSTEM (June, 1991), http://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html ("(b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License").

41. Consider, e.g., the varied licensing terms of SAP PRODUCT STEWARDSHIP NETWORK LICENSES http://go.sap.com/product/plm/product-stewardship-network.licensing-purchasing.html.

42. The first mover advantage is a very market-centric analysis and subject to many exceptions. Consider, Fernando Suarez & Gianvito Lanzolla, *The Half-Truth of First-Mover Advantage*, HARV. BUS. REV., (Apr. 2005), https://hbr.org/2005/04/the-half- truth-of- first-mover- advantage.

by virtue of the noncompliance (e.g., repurposing an already existing open source solution rather than developing its own from scratch). Being forced to now comply, after the competition is gone, would do little to raise *Disclosure_Cost*$_{\Pi A}$, unless that competition returns.

If this is the situation, **Δ** should identify competitors and new entrants who may be able to take advantage of **Π**$^{\mathbf{A}}$'s forced compliance via injunction. A competitor who may have "given up" may now find that it has the advantage by virtue of its (mistakenly) late-to-market, proprietary solution which does not rely upon the open source component. Where **Π**$^{\mathbf{A}}$'s product is not purely software (e.g., firmware or hardware), **Δ** can be somewhat more confident that this market displacement has less insulating effect (though this will depend upon the context).[43] In any event, if this insulating effect is large, **Δ** should consider whether antitrust actions, or unfair business competition actions, will suffice to return *Disclosure_Cost*$_{\Pi A}$ to its pre-insulation value.

b. Monetary Relief

As discussed above in relation to *Jacobsen v. Katzer*, the most common remedy for an open source violation may be injunctive relief. As the software was generally available for "free", permissive open source licenses will typically result in few, if any, monetary damages for copyright infringement, save the possibility of some statutory damages.[44] To achieve substantial monetary damages under the copyright, tortious interference with business relations, antitrust, and other causes of action, **Π**$^{\mathbf{B}}$ must operate its business such that **Π**$^{\mathbf{A}}$'s abuse of the license resulted in a tangible profit loss to **Π**$^{\mathbf{B}}$.

Π$^{\mathbf{B}}$'s profit loss may occur in several ways. Certainly, unfair competition may present opportunities for monetary damages in the form of lost profits, though **Δ** should consider what **Π**$^{\mathbf{B}}$ will need to prove to demonstrate this market loss.[45] Where **Π**$^{\mathbf{B}}$ offered the open source software under a "dual license" allowing licensees to accept the software under either the open source license or a commercial license, the monetary damages may

43. *Id*. While not a universal rule, such products are often subject to slower change, and consequently in the "calmer waters" referenced in this article.

44. Statutory damages require that **Π**$^{\mathbf{B}}$ have the foresight to register their work and provide $750 to $30,000 per infringement of the work and an additional $150,000 for willful infringement. *See*, 17 U.S.C. §504(c) (1947). However, statutory damages will often not be the best vehicle for increasing *Disclosure_Cost*$_{\Pi A}$, as the damages are calculated based upon the number of copyrighted works and number of infringers, but *not* the number of incidents of infringement. *See, e.g.*, Fitzgerald v. CBS Broad., Inc., 491 F. Supp. 2d 177, 182 (D. Mass. 2007).

45. *See, e.g.*, Cal. Civ. Code, § 3345(b) (unfair competition law is one in which the trier of fact "is authorized by statute to impose a fine, or a civil penalty or other penalty, or any other remedy the purpose or effect of which is to punish or deter . . ."); *See also*, Bank of the West v. Superior Court 2 Cal.4th 1254, 1267 (1992) (indicating that the remedy may have a "deterrent purpose and effect").

be more certain.[46] **Π^A**'s failure to take either license in this scenario, will likely result in a quantifiable unjust enrichment to **Π^A** or lost profits to **Π^B**.

Reputational harm may itself precipitate financial consequences to **Π^A**, even when remediation is *de minimis*. Indeed, in some communities, callous failure to comply with *de minimis* obligations may result in reputational harm *because* they are *de minimis*.[47] This reputational harm may precipitate customer departures and jeopardize **Π^A**'s participation in future open source projects.[48] In this respect, to the extent that **Δ** can influence media attention and otherwise call attention to the breach, **Δ** may be able to increase **Π^A**'s perception of $Disclosure\_Cost_{\Pi A}$.[49]

2. New Counterclaims **B1**

In some situations, disclosure may permit **Δ** additional counterclaims against **Π^A** that may increase $Disclosure\_Cost_{\Pi A}$. **Δ**'s ability to bring additional counterclaims depends upon the character of the open source deficiency and **Δ**'s relationship to **Π^A**. For example, as previously discussed, **Δ** may assert that it was the third party beneficiary of a copyleft open source license, particularly where there was an obligation to disclose source code or provide specific terms to downstream recipients (indeed, as discussed in the footnotes, such a counterclaim may be necessary to prevent the threat's characterization as extortion).

Where **Δ** is a customer of **Π^A**, **Π^A** may have required **Δ** to indemnify **Π^A** or to disclaim liability for open source noncompliance. Even in these

46. For example, in Oracle America v. Google, 750 F.3d 1339, 1377 (Fed. Cir. 2014), Oracle provided the Java API under either the GPL open source license or a commercial license. Arguably, in this situation, a customer's unwillingness to comply with the GPL's restrictive character, or to take a commercial license, reduced the market for the commercial license (even if the customer were willing to comply with the GPL a downstream customer may have preferred the commercial license). *See* Exhibit G, Oracle America v. Google, 750 F.3d 1339 (Fed. Cir. 2014) (No. 1571-8) 3:10-cv-03561 ("I determined that Oracle's lost profits from lost Java ME license agreements with third parties totaled $475 million."). This argument, however, requires that the circumstances and licensing environment encourage such an either-or behavior between the open and commercial license.

47. Consider the example of *Jacobsen v. Katzer* ("The software underlying such an important legal dispute is almost charmingly inconsequential from a commercial point of view - model railroad software. But to the litigants, the stakes were high relative to their resources and their commitment to that niche. The plaintiff, Robert Jacobsen, is a software developer member of the Java Model Railroad Interface (JMRI) Project, and the defendant, Matthew Katzer, is the owner of a proprietary vendor of model train software called KAMIND associates, d/b/a KAM Industries.") Andy Updegrove, *A Big Victory for F/OSS: Jacobsen v Katzer is Settled*, THE STANDARDS BLOG (Feb. 19, 2010), http://www.consortiuminfo.org/standardsblog/article.php?story=201002190850472.

48. Such participation may often be part of a business strategy, e.g., in a "razor / razor-blade" business model.

49. For example, a court would generally be unlikely to entertain a criminal allegation under the DMCA against an open source violation, but the public media and community consequences following from such an accusation may suffice to raise $Disclosure\_Cost_{\Pi A}$.

circumstances, however, disclosure may provide the evidentiary basis for **Δ** to bring an antitrust action.[50] Such an action's effectiveness will depend upon the market posture of the parties. As discussed in the following section, **Δ** may seek to align its post-disclosure position with **C** as much as possible, or at least cause $\mathbf{\Pi^A}$ to perceive as much, to increase the apparent value of $Disclosure\_Cost_{\Pi A}$.

Still, in most contexts, it is unlikely that **B1** will be the primary basis for increasing $Disclosure\_Cost_{\Pi A}$, because **Δ** is neither the copyright owner nor the market participant originally motivated to develop the open source software.[51] Instead, as discussed in greater detail below, if **Δ** acquires the copyright to the open source component from $\mathbf{\Pi^B}$, **Δ** may subsume **C1**, **C2**, and **C3** within **B1** so as to maximize $Disclosure\_Cost_{\Pi A}$.

3. Pressures from Downstream Customers **D1**

$\mathbf{\Pi^A}$'s awareness of the consequent **D1** pressures will increase $Disclosure\_Cost_{\Pi A}$. As **D1** directly follows from the character of **C3** (e.g., the resultant pressures when, and if, customers become subject to an injunctive order) **Δ** may analyze **C3** as a proxy for **D1** to a certain extent. To this end, **Δ** should consider if and how $\mathbf{\Pi^B}$ will bring **C3**. Some $\mathbf{\Pi^B}$s may simply ignore **C**, not wishing to suffer reputational harm in the community by suing end customers (e.g., where $\mathbf{\Pi^B}$ is an educational nonprofit). Conversely, some $\mathbf{\Pi^B}$s may have no choice but to pursue action against **C** (e.g., where $\mathbf{\Pi^B}$ is a large corporation whose shareholders and board compel directors to recapture lost profits). In some instances, **C3** may not be present, depending upon the customer behavior.[52] Accordingly, **Δ** should consider the character of $\mathbf{\Pi^B}$ when analyzing **C3** and, in turn, **D1**.

$\mathbf{\Pi^A}$ will likely have indemnified itself or disclaimed any warranty regarding copyright infringement in its agreements with customers **C**.

50. Section 43(a) of the Lanham Act provides that any "false designation of origin, false or misleading description of fact, or false or misleading representation of fact –(a) which is likely to cause confusion, or to cause mistake" is illegal. 15 U.S.C. § 1125 (2012). The defendant may seek damages and an injunction. Additionally, Section 4 of the Clayton Act 1914 allows for the recovery of damages by "any person injured in his business or property by reason of anything forbidden in the antitrust laws" 15 U.S.C. 15(a) (2012). The claimant need merely demonstrate that "injury of the type the antitrust laws were intended to prevent and that flows from that which makes defendants' acts unlawful" Brunswick Corp. v. Pueblo Bowl-O-Mat Inc., 429 US 477, 489 (1977).

51. Again, as mentioned elsewhere herein, a third party beneficiary counterclaim's greatest value may be in mitigating extortion allegations, effectively reducing $Disclosure\_Cost_{\Delta}$. *See, e.g.*, U.S. v. Pendergraft, 297 F.3d 1198, 1204 (11th Cir. 2002) ("Generally, a threat to file a lawsuit, even if made in bad faith, does not constitute extortion).

52. For example, internal use and distribution does not trigger the copyleft obligations of many otherwise onerous licenses, such as the GPL license. If the customers are not themselves distributing infringing versions, but merely using internal copies, $\mathbf{\Pi^B}$ may have no credible basis for bringing an action against them.

Prudent **C**s will have stipulated to these terms only subject to proper open source diligence, representations and warranties, etc. by $\mathbf{\Pi^A}$. The transaction costs involved in litigating these provisions, even if simply to establish that they are enforceable, may contribute to *Disclosure_Cost*$_{\Pi A}$. **C**s who have not taken such precautions may still exert considerable pressure by selecting an alternative provider than $\mathbf{\Pi^A}$. Since **Δ** may not know the character or scope of **C** and **C**'s agreement with $\mathbf{\Pi^A}$, **Δ** should make clear to $\mathbf{\Pi^A}$ that it will apprise $\mathbf{\Pi^B}$ of *as many* **C**s as possible if it discloses. Accordingly, any customer lists uncovered during **A1**'s discovery, which are not subject to a protective order, may be especially useful in this regard (See Section II.C.2.b below). Naturally, however, such behavior is more likely to be condemned in a protective order or in action seeking to determine that **Δ**'s threat constitutes extortion (e.g., that it was "wrongful" by the terms of some extortion laws).

In some instances, $\mathbf{\Pi^A}$ and **Δ** may share customers within **C**. In these circumstances, **Δ** should consider whether **C3** would simply provide **Δ** greater market share, or would alienate customers **C** against **Δ**. This alienation may be particularly acute if the **C**s learn that **Δ** was the source of the disclosure to $\mathbf{\Pi^B}$. Accordingly, **Δ** may preemptively notify shared customers **C** and provide them with an opportunity to comply/remediate, before making the threat to $\mathbf{\Pi^A}$. Naturally, the timing and character of such a warning will depend upon **C**'s capacity to remediate, and **Δ**'s concern that **C** will prematurely warn $\mathbf{\Pi^A}$. Such premature warning may cause $\mathbf{\Pi^A}$ to acquire the copyright from $\mathbf{\Pi^B}$ before **Δ** has had a chance to make its own offer. Consequently, if **Δ** is considering purchasing the copyright from $\mathbf{\Pi^B}$ (discussed in detail below in Section II.C.1), **Δ** should make its purchase attempt before issuing a warning to any of **C**.

*C. Influencing **A1** - "How Should Δ Threaten"?*

As the threat's effectiveness depends upon $\mathbf{\Pi^A}$'s perception of Conditions 1 and 2 being true, the manner in which **Δ** poses the threat is of considerable importance. Certainly, **Δ**'s characterization of each of the parameters in Conditions 1 and 2 will influence $\mathbf{\Pi^A}$ as they will make the threat more credible. But the goal is not simply to make $\mathbf{\Pi^A}$ feel threatened, but to compel $\mathbf{\Pi^A}$ to abandon **A1**. If **Δ** loses sight of this broader goal, posing the threat indelicately, $\mathbf{\Pi^A}$ may assume **Δ** intends to enter a state of total war. $\mathbf{\Pi^A}$ may begin remediating the violation or seek to acquire the open source copyright from $\mathbf{\Pi^B}$, without considering whether dropping **A1** would instead be more economical. Anticipating this scenario, **Δ** must consider the likelihood of $\mathbf{\Pi^B}$'s consenting to sell the copyright to $\mathbf{\Pi^A}$ before making the

threat to **Π^A**. In some circumstances, for example, where such a sale to **Π^A** is likely, **Δ** may seek to preemptively acquire **Π^B**'s copyright itself before making the threat.

1. Acquiring the Copyright

Many circumstances will compel **Δ** to attempt to acquire **Π^B**'s copyright in the open source software. If **Π^B**'s purchase price is low, if $Disclosure\_Cost_{\Delta}$ is unacceptably high, or if it is unlikely that **Π^B** will take action against **Π^A** or **C**, then **Δ** should attempt to acquire ownership of **Π^B**'s copyright before posing the disclosure threat to **Π^A**.[53] Naturally, **Δ** will probably make the offer through an intermediary so that **Π^B** does not infer **Π^A** or **Δ**'s noncompliance. Such an inference may cause **Π^B** to increase its asking price or to initiate action before **Δ** has made its threat to **Π^A**. How much should **Δ** be willing to offer **Π^B**? If **Π^B** rejects **Δ**'s offer, should **Δ** be concerned that **Π^B** will accept **Π^A**'s offer after **Δ** threatens **Π^A**? The following section considers each party's ability to acquire the copyright (their "purchase price capacity") to answer these questions.

a. Purchase Price Capacity

Figure 3 generally illustrates **Δ** and **Π^A**'s relative purchase price capacities (shaded regions) for **Π^B**'s open source copyright.

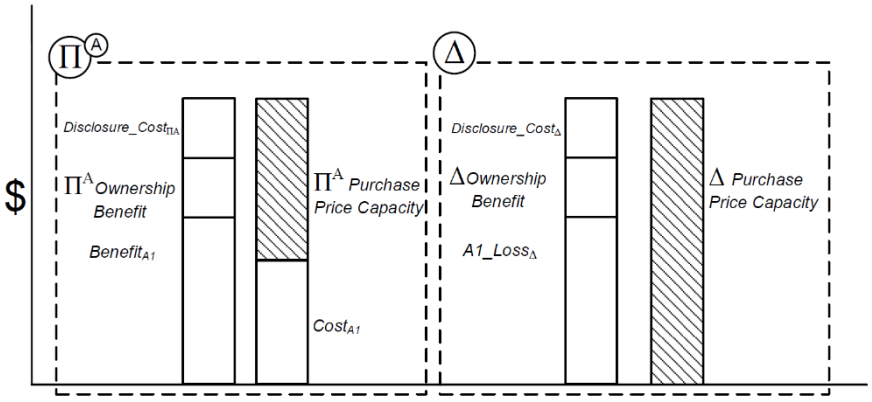

FIGURE 3: Purchase Price Capacity

53. *N.B.*, however, that **Δ**'s acquiring the copyright may remove some of the antitrust and tortious interference causes of action discussed above as it was **Π^B** and not **Δ** who suffered theses harms. In these situations, **Δ** may attempt to involve **Π^B** in the action for those causes which **Δ** cannot avail itself to increase $Disclosure\_Cost_{\Pi A}$.

Figure 3 is simply a graphical representation of the following pseudo-algebraic Equations 7 and 8:[54]

$$\begin{aligned}\boldsymbol{\Pi}^{\boldsymbol{A}}_{Purchase\ Price\ Capacity} = \mathrm{Max}(0, &Benefit_{A1} \\ &+ \boldsymbol{\Pi}^{\boldsymbol{A}}_{Ownership\ Benefit} \\ &+ Disclosure\_Cost_{\Pi A} \\ &-\mathrm{Cost}_{A1}\ )\end{aligned} \tag{7}$$

$$\begin{aligned}\boldsymbol{\Delta}_{Purchase\ Price\ Capacity} = &A1_{Loss_{\Delta}} \\ &+ \boldsymbol{\Delta}_{Ownership\ Benefit} \\ &+ Disclosure\_Cost_{\Delta}\end{aligned} \tag{8}$$

$\boldsymbol{\Pi}^{\boldsymbol{A}}_{Ownership\ Benefit}$ and $\boldsymbol{\Delta}_{Ownership\_Benefit}$ reflect the secondary, incidental benefits accruing to each party after the purchase.[55] This may include the party's new ability to sue the other for copyright infringement (e.g., the ability to apply **C1** or **C2**). Generally, $\boldsymbol{\Pi}^{\mathbf{A}}$ should be willing to pay as much as necessary to retain the benefit of **A1** and to gain any incidental benefits that accompany copyright ownership ($\boldsymbol{\Pi}^{\boldsymbol{A}}_{Ownership\ Benefit}$), as well as to avoid $Disclosure\_Cost_{\Pi A}$ (addition provides a straightforward way to assess the relation, but one will recognized that many real-world situations will involve more nuanced relationships). As previously discussed, the benefit of **A1** to $\boldsymbol{\Pi}^{\mathbf{A}}$ is already offset by the cost $Cost_{A1}$. Thus, the remainder is the maximum price $\boldsymbol{\Pi}^{\mathbf{A}}$ would be willing to pay to own $\boldsymbol{\Pi}^{\mathbf{B}}$'s copyright ($\boldsymbol{\Pi}^{\mathbf{A}}$'s purchase price capacity). $\boldsymbol{\Pi}^{\mathbf{A}}$ would be unreasonable to pay $\boldsymbol{\Pi}^{\mathbf{B}}$ more than this amount.

Δ's analysis is similar. If **Δ** is committed to make the disclosure, then purchasing the copyright will permit **Δ** to (hopefully) close out **A1** to avoid $A1\_Loss_{\Delta}$, to avoid $Disclosure\_Cost_{\Delta}$, and to receive any incidental benefits that accompany copyright ownership $\boldsymbol{\Delta}_{Ownership\_Benefit}$ (such as suing $\boldsymbol{\Pi}^{\mathbf{A}}$). Unlike $\boldsymbol{\Pi}^{\mathbf{A}}$, **Δ**'s costs defending **A1** are part of $A1\_Loss_{\Delta}$ which contribute to **Δ**'s purchase price capacity, while $\boldsymbol{\Pi}^{\mathbf{A}}$'s costs pursuing **A1** detract from $\boldsymbol{\Pi}^{\mathbf{A}}$'s purchase price capacity. Thus, all other things being equal, **Δ** may have a

54. While pseudo-algebraic one could infer actual dollar amounts from these considerations.

55. For example, where the open source license was offered under a dual commercial license, or where it permits the owner to influence its development. Naturally, such benefits may also include **Δ** or $\boldsymbol{\Pi}^{\mathbf{A}}$'s ability to "step in" $\boldsymbol{\Pi}^{\mathbf{B}}$'s shoes and bring a new cause of action against the other (e.g., **C1** or **C2**).

slight bargaining advantage over $\mathbf{\Pi^A}$ (as illustrated in the arbitrary values of Figure 3).

Δ also has a slight advantage in that it can make an offer to $\mathbf{\Pi^B}$ *before* $\mathbf{\Pi^A}$. This will provide **Δ** with an opportunity to "prime" $\mathbf{\Pi^B}$ before $\mathbf{\Pi^A}$ can make its offer (additionally, **Δ** has the benefit of making its offer without $\mathbf{\Pi^A}$ having primed $\mathbf{\Pi^B}$). Priming permits a party to establish a pricing reference point that influences subsequent negotiations.[56] This priming advantage may manifest itself most acutely if it becomes clear that $\mathbf{\Pi^B}$ will not sell to **Δ** during their negotiations. Once this is clear, **Δ** will likely begin making outrageous offers to $\mathbf{\Pi^B}$, with no real intention of fulfillment, expecting that $\mathbf{\Pi^B}$ will consider its preceding refusal of these offers when $\mathbf{\Pi^A}$ makes its own offer (e.g., causing $\mathbf{\Pi^B}$ to ignore an otherwise reasonable offer from $\mathbf{\Pi^A}$). **Δ**'s first mover advantage also manifests itself in **Δ**'s ability to encourage $\mathbf{\Pi^B}$ to litigate before $\mathbf{\Pi^A}$ can make its offer. Particularly, if it again becomes clear that $\mathbf{\Pi^B}$ will not sell to **Δ**, then **Δ** may let $\mathbf{\Pi^B}$ know of the *existence* of a noncompliant licensee, without divulging that the licensee's identity is $\mathbf{\Pi^A}$. This knowledge may cause $\mathbf{\Pi^B}$ to prepare for litigation, particularly where such noncompliance has clearly resulted in a market loss to $\mathbf{\Pi^B}$. If $\mathbf{\Pi^B}$ does not submit to **Δ**'s threat, **Δ** will immediately inform $\mathbf{\Pi^B}$ of $\mathbf{\Pi^A}$'s breach, attempting to deprive $\mathbf{\Pi^B}$ of a negotiation opportunity before $\mathbf{\Pi^A}$ and $\mathbf{\Pi^B}$ enter a state of conflict.

Despite these advantages, the prices $\mathbf{\Pi^A}$ and **Δ** are willing to pay for the copyright will probably be the determining factor in $\mathbf{\Pi^B}$'s decision to sell. That some of the parameters influencing pricing are the same parameters in the threat credibility conditions can affect negotiations in interesting ways. For example, consider when **Δ** is making its threat to $\mathbf{\Pi^A}$. Initially, **Δ** should emphasize to $\mathbf{\Pi^A}$ how great $Disclosure\_Cost_{\Pi A}$ is, and how small $Disclosure\_Cost_{\Delta}$ is, so that $\mathbf{\Pi^A}$ is convinced that Conditions 1 and 2 are true. If it becomes apparent that the threat has been ineffective, though, such arguments may have instead simply convinced $\mathbf{\Pi^A}$ that it should be willing to pay a higher price than **Δ** for the copyright (see Figure 3). At this point, **Δ** may be unwise to simply backtrack and convince $\mathbf{\Pi^A}$ of the opposite view, as confessing that $Disclosure\_Cost_{\Delta}$ is in fact quite large may simply raise $\mathbf{\Pi}^{\boldsymbol{A}}_{Ownership\ Benefit}$. Instead, **Δ** will likely retract its high assessment of

56. See, e.g., Paul Herr, *Priming Price: Prior Knowledge and Context Effects*, 16 J. OF CONSUMER RES. 67, 68 (Jun. 1989) ("Although priming can produce these judgmental and behavioral effects, what interests many is its often passive nature (see especially Higgins, Bargh, and Lombardi, *Nature of Priming Effects on Categorizations*, 11 J. EXPERIMENTAL PSYCHOL. 59 (1985). Subjects do not necessarily consciously compare the stimulus to the primed category.").

Disclosure_Cost$_{\Pi A}$ while spurring $\mathbf{\Pi^B}$ to litigate before $\mathbf{\Pi^A}$ can make its own offer.

To help conceptualize how parameter variations can influence the parties' respective purchase prices, consider Figures 4 and 5.

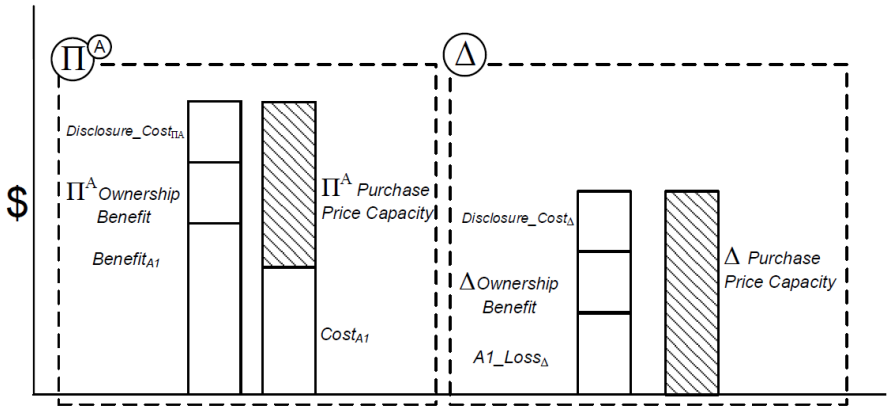

FIGURE 4: Example Variation "Little *A1_Loss*$_{\Delta}$"

Figure 4 illustrates a situation where **Δ** can make a purchase price offer competitive with $\mathbf{\Pi^A}$'s offer, even when *A1_Loss*$_{\Delta}$ is "low". Generally, such situations will be possible because, as mentioned previously, **Δ**'s ability to forego its **A1** litigation costs contribute to its purchasing capacity (since owning the copyright will avoid these costs if **A1** is settled) while $\mathbf{\Pi^A}$'s **A1** litigation costs detract from its purchasing capacity (since those costs must still be incurred to gain the benefit of **A1**).

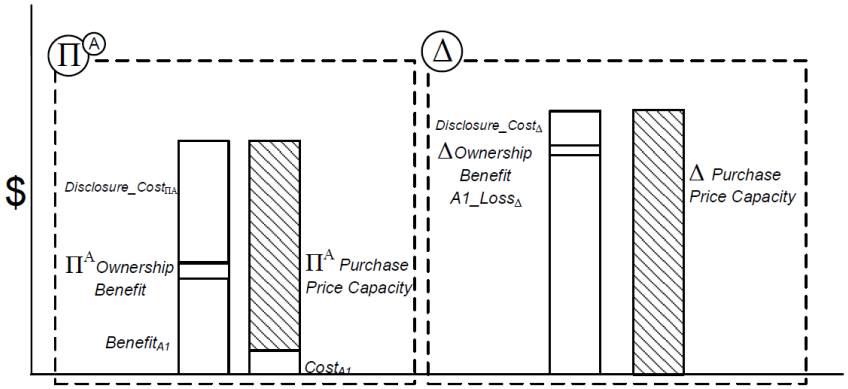

FIGURE 5: Example Variation "Great *A1_Loss*$_{\Delta}$"

Figure 5 considers a situation where $\mathbf{\Pi^A}$ brought **A1** punitively (i.e., primarily designed to harm **Δ** rather than benefit $\mathbf{\Pi^A}$). For example, large corporate conglomerates have sometimes found it effective to incur great short-term losses to outcompete a new, small market entrant.[57] This may result in long-term benefits to the conglomerate by discouraging future entrants in other markets.[58] Consequently, depending on how confident the conglomerate is in its long-term strategy, the goal may not be to incur a large $Benefit_{A1}$, but simply to cause a large $A1\_Loss_{\Delta}$. A large $A1\_Loss_{\Delta}$, however, may compel the small entrant to pay a much larger price than $\mathbf{\Pi^A}$ for $\mathbf{\Pi^B}$'s copyright as illustrated in the figure. As illustrated in Figure 5, $\mathbf{\Pi^A}$ may not be willing to pay a higher price *even when* **Δ**'s ownership of the copyright will compel $\mathbf{\Pi^A}$ to abandon **A1**.[59] Additionally, by forcing the conglomerate to consider how much it would pay for the open source component, the smaller entrant may compel the conglomerate to evaluate the discounted present value of its deterrence program – an exercise the conglomerate may not otherwise have bothered to perform.

b. Demonstrating Commitment - Failed Purchase

What if **Δ** is unable, or unwilling, to purchase $\mathbf{\Pi^B}$'s copyright and knows that both it and $\mathbf{\Pi^A}$ will be subject to devastating suits from $\mathbf{\Pi^B}$ (i.e., Condition 2 is unsatisfied)? Can **Δ** still make a convincing threat to $\mathbf{\Pi^A}$ even when the disclosure will ensure **Δ**'s own destruction or near-destruction?

Often, yes. Game theory (and common sense) have long recognized that situations involving mutual destruction or near-destruction may be the basis for unilateral threats by demonstrating either: 1) a greater risk tolerance; or 2) commitment. With regard to risk tolerance, **Δ** can give $\mathbf{\Pi^A}$ the impression that $A1\_Loss_{\Delta}$ is much higher than it really is. Pursuant to Condition 2, this will compensate for an increased $Disclosure\_Cost_{\Delta}$ making the threat credible again. **Δ** may also demonstrate a higher risk tolerance by including a counterclaim threat with the disclosure threat that will escalate **A1** (e.g., initiating reciprocal patent infringement actions). This would likewise have the same effect as raising A_Loss_{Δ}.

57. Rightly or wrongly, large organizations are often compelled to adopt aggressive tactics against smaller retailers (*See, e.g.*, Drew Sandholm, *Amazon's 'Predatory Pricing' Questioned*, CNBC (Jun. 30, 2014), http://www.cnbc.com/2014/06/30/amazons-predatory-pricing-questioned.html). Smaller retailers are then themselves compelled to respond with creative countermeasures such as the compliance-based tactics discussed herein.

58. The author understands that such strategies are not considered economic "dumping" as a matter of relative degree.

59. To clarify, in the example of Figure 5, $Cost_{A1}$ and $Disclosure\_Cost_{\Pi A}$ together are greater than $Benefit_{A1}$.

With respect to commitment, **Δ** can inform **Π^{A}** tacitly, or directly, that it has denied itself the ability to back out of the threat (effectively reducing $C_{context}$ for Condition 2). For example, consider where **Δ** begins the threat to **Π^{A}** with the following "dead switch" disclosure statement: "I have instructed a third party trustee to disclose everything I am about to tell you to **Π^{B}** unless the trustee hears of our settlement in a public news statement by the end of tomorrow. I have already paid the trustee and the trustee is now unreachable by any means other than that public news statement".[60] Assuming, **Π^{A}** believes that **Δ** is telling the truth (which may be demonstrated by a variety of means), **Δ** will have effectively eliminated Condition 2 from **Π^{A}**'s consideration.

Effectively combining risk tolerance and commitment, **Δ** can also try to convince **Π^{B}** that **Δ** is irrational. As discussed in greater detail in the footnote, if **Δ** can credibly present the violation's disclosure to **Π^{A}** as a "ticking time bomb", the suppression of which is only partially within **Δ**'s control, then **Π^{A}** will be more likely to acquiesce.[61]

2. **Δ**'s Ability to Notify **Π^{B}**

Until now, the analysis has generally assumed that **Δ** has the ability to disclose **Π^{A}**'s breach to **Π^{B}** at **Δ**'s discretion. This may not be the case.[62] Consider the three factual variations:

60. Thomas Schelling, *An Essay on Bargaining*, 46 AM. ECON. REV. 281, 283 (Jun. 1956)(See discussion regarding "cross my heart" commitment). Thomas Schelling, *supra*, "An Essay On Bargaining" ("[I]f the buyer can accept an **irrevocable commitment**, in a way that is **unambiguously visible** to the seller, he can squeeze the range of indeterminacy down to the point most favorable to him," emphasis added). Certainly, such a theatrical entrance would align with an extortion allegation, but as discussed previously, **Δ** may attempt to mitigate this risk by subsuming its behavior under the right of a third party beneficiary counterclaim (even if **Δ**'s threat to disclose to **Π^{B}** were construed as extortion, **Δ** could simply recharacterize the threat as the bringing of the counterclaim which would itself indirectly notify **Π^{B}**). This theatrical example could accordingly be re-characterized to this end, e.g.: "I have instructed my attorney trustee to file a counterclaim . . ." etc.

61. Michael Kinsley, *A Nobel Laureate Who's Got Game*, WASHINGTON POST (Oct. 11, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/10/11/ AR2005101101336.html.

> So you're standing at the edge of a cliff, chained by the ankle to someone else. You'll be released, and one of you will get a large prize, as soon as the other gives in. How do you persuade the other guy to give in, when the only method at your disposal—threatening to push him off the cliff—would doom you both?
>
> Answer: You start dancing, closer and closer to the edge. That way, you don't have to convince him that you would do something totally irrational: plunge him and yourself off the cliff. **You just have to convince him that you are prepared to take a higher risk than he is** of accidentally falling off the cliff. If you can do that, you win (emphasis added).

62. Note that this discussion concerns the ability <u>to disclose</u>, not the ability <u>to threaten</u>. "Extortion has been characterized as a paradoxical crime in that it criminalizes the making of threats that, in and of themselves, **may not be illegal**." Flatley v. Mauro, 39 Cal.4th 299, 326, 46 Cal.Rptr.3d 606, 627, 139 P.3d 2, 19-20 (2006) (emphasis added). **Π^{A}** may try to raise *Disclosure_Cost*$_{\Delta}$ by intimating or bringing (in jurisdictions where applicable) allegations of extortion after **Δ** has made its threat. E.g., In California, "Extortion is the **obtaining of property** from another, with his consent . . . induced by a **wrongful use** of force or fear . . ." CAL. PENAL CODE, § 518 (emphasis added). Fear, for purposes of extortion "may be

(a) **Δ** discovers **ΠA**'s noncompliance independently of any nondisclosure obligation (e.g., **Δ** discovers the noncompliance during **A1** discovery when there is no protective order in place); or

(b) **Δ** discovers **ΠA**'s noncompliance but is subject to a nondisclosure obligation (e.g., a prior contractual nondisclosure agreement with **ΠA** or a protective discovery order); or

(c) **ΠB** becomes aware of **ΠA**'s noncompliance independent of any action by **Δ** (e.g., by luck or from a whistleblower within **ΠA**'s organization)

Note that (a), (b), and (c) are not necessarily mutually exclusive. For example, (a) may be true before litigation occurs, then (b) may be true once a protective order issues during litigation, and then (c) may occur independently of **A1** (e.g., by coincidence). The following sections consider these situations in turn.

a. Fact Pattern (a) – Δ Recognizes Breach Independently of Litigation or Any Restrictive Obligation

For the breach to be "independent of the litigation or any restrictive obligation", **Δ** should be at liberty to disclose the breach at any time of **Δ**'s choosing. This would mean that **Δ** is under no obligation, e.g., via a license from **ΠA** or by a protective order during discovery, which prevents such disclosure. License provisions preventing **Δ** from disclosing violations to **ΠB** are discussed in greater detail below. **Δ**'s circumstance will most often accord with this fact pattern (a), as **ΠA**'s software will often already be publicly accessible or at least subject to reverse engineering.

induced by a threat, either: . . . 2. To accuse the individual threatened . . . of any crime; or, 3. To expose, or impute to him . . . any deformity, disgrace or crime" (CAL. PENAL CODE, § 519). While a compelled settlement of **A1** might be construed as "the obtaining of property", it's less clear that the contemplated disclosure would be "wrongful". As previously mentioned, if **Δ** can subsume its threat within its third party beneficiary rights, those rights may obviate claims of extortion. *See, e.g.,* U.S. v. Pendergraft, 297 F.3d 1198, 1204 (11th Cir. 2002) ("Generally, a threat to file a lawsuit, even if made in bad faith, does not constitute extortion") for a federal rather than state extortion discussion.

Note that as extortion is only a criminal statute in many jurisdictions, civil remedies may not be available to **ΠA**, though a successful demonstration of extortion may suffice to nullify the resulting settlement agreement. Where civil remedies are not available **ΠA** may be able to introduce extortion as a predicate basis for alleging a RICO claim, *See, e.g.,* DIRECTV, Inc. v. Cavanaugh, 321 F. Supp. 2d 825, 834 (E.D. Mich. 2003).

Some jurisdictions, such as California, do recognize a civil common law cause of action for extortion, but it's unclear that the disclosure in question fits the pattern exemplified by this case law. For example, the common law version appears to require that the threat maker know that the crimes it will threaten to disclose are untrue. *See, e.g.*, Fuhrman v. California Satellite Systems 179 Cal. App. 3d 408, 426 (1986) (The Court overruled on other grounds ("To be actionable the threat of prosecution must be made with the knowledge of the falsity of the claim", citing Leeper v. Beltrami, 53 Cal.2d 195, 204 (1959)); *See also*, Cohen v. Brown, 173 Cal. App. 4th 302 (2009).

Because this freedom affords the greatest bargaining power, litigious **Δ**s or **Δ**s fearing litigation may proactively seek to identify their competitor's violations before entering into a license with **Π^{A}** and well in advance of anticipated litigation. The former will permit **Δ** to retain the benefit of knowledge of the violation (assuming its discovery is properly documented), while still binding itself to any forward-looking restriction. The latter will permit **Δ** to avoid any restrictions imposed during discovery, discussed below.

b. Fact Pattern (b) – Δ Recognizes Breach During Litigation Discovery

Δ's ability to disclose a violation uncovered during discovery will depend upon the discovery context. While the public has an interest in reviewing court filings, courts often temper that interest (to varying degrees) based upon the parties' interests.[63] Anticipating this, an aggressive **Π^{A}** may try to isolate documents related to potential breaches by requesting a protective order in response to any of **Δ**'s discovery requests.[64] This is hardly a fool-proof defense, however. **Δ**'s discovery request may itself enter the public record and encourage third party exploration of **Π^{A}**'s code.[65] Where a

63. In California, the issuance and formulation of protective orders are to a large extent discretionary. *See, e.g.,* Coalition Against Police Abuse v. Superior Court, 170 Cal. App. 3d 888, 904 (Cal. App. Ct. 1985). **Π^{A}**'s task is somewhat further complicated by the fact that most federal circuits recognize a public interest in the sharing of information uncovered during discovery.

> "In Olympic Refining the Ninth Circuit established the principle which has remained the rule in this and virtually all other circuits ever since." (Kraszewski, supra, 139 F.R.D. at p. 159.) **This rule allows sharing of information in similar cases in order to ease the tasks of courts and litigants in the discovery process** . . ." (emphasis added) (Fn. Omitted.) (Olympic Refining Company, supra, 332 F.2d at p. 265.)

Π^{A} may seek to keep the violation confidential by preventing the appearance of software in the record. Particularly, "the majority of courts, both state and federal, do not recognize a public right of access to materials that parties exchange in discovery **but do not file with the court**." Andrew D. Goldstein, *Sealing and Revealing: Rethinking the Rules Governing Public Access to Information Gathered Through Litigation*, 81 CHI.-KENT L. REV. 375, 376 (2006) (emphasis added). *See also,* Estate of Frankl v. Goodyear Tire & Rubber Co., 853 A.2d 880, 886-87 (N.J. 2004) ("The universal understanding in the legal community is that unfiled documents in discovery are not subject to public access.") Such rules will, however, vary between jurisdictions; *See also* SEC v. TheStreet.com, 273 F.3d 222, 233 n. 11 (2d Cir. 2001) ("[T]o the extent that Agent Orange relied upon Federal Rule of Civil Procedure 5(d) to find a statutory right of access to discovery materials, we observe that the recent amendment to this rule provides no presumption of filing all discovery materials, let alone public access to them."); *In contrast, see e.g.,* San Jose Mercury News, Inc. v. U.S. Dist. Ct., 187 F.3d 1096, 1101 (9th Cir. 1999) ("The right of access to court documents belongs to the public, and the Plaintiffs were in no position to bargain that right away.").

64. FRCP Rule 26 provides for protective orders ("(1) In General. A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending—or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken."). FED. R. CIV. P. 26(c)(1).

65. Suspicion can be aroused in a number of ways – even a request by **Δ** for documents related to open source records that **Δ** knows will be denied may suffice to arouse the suspicion of a copyright owner such that they begin their own investigation. Indeed, because **Π^{A}**'s product is typically otherwise publicly

protective order issues, the court may be limited in the sanctions it can impose for its breach.[66] Certainly, given how little **Δ** need say or suggest to **ΠB** for **ΠB** to infer the threat, the court may have difficulty establishing that **Δ** violated the order, let alone determining what sanctions would be proportional.[67] Consequently, the sanctions may do little to increase *Disclosure_Cost*$_{\Delta}$. Accordingly, a more proactive **ΠA** may instead prefer a contractual remedy as discussed in Section III, when **Δ** was a previous customer.

*c. Fact Pattern (c) – **ΠB** Recognizes Breach Independently of **ΠA**-**Δ** Litigation*

As timing is a critical factor in the effectiveness of **Δ**'s threat presentation, premature action by the copyright holder can severely mitigate the tactic's effectiveness. Certainly, if **ΠB** asserts its rights before **Δ** has a chance to threaten **ΠA** with the disclosure, the tactic will be unusable. Still, it may be in **Δ**'s interests to acquire the copyright AFTER **ΠB** has discovered the breach. Certainly, this will likely be difficult, as **ΠB** will be able to then infer the value of the copyright to **Δ** and **ΠA** from the action.[68] Still, **ΠB**'s price may change as each of the respective litigations progress and so the parties may revisit purchasing negotiations as their interests fluctuate.

III. COUNTERING COMPLIANCE-BASED DEFENSE TACTICS

This section provides general guidance for how **ΠA** may deny **Δ** use of the tactics discussed above. Certain countermeasures are already apparent

accessible, it will be difficult for **ΠA** to demonstrate that **Δ**'s breach of a protective order was the "but-for" cause for an independent investigation.

66. Adam M. Josephs, *The Availability of Discovery Sanctions for Violations of Protective Orders*, 80 UNIV. CHICAGO L. REV. 1355, 1356-57 (2013) ("Rule 37(b) of the Federal Rules of Civil Procedure, which allows for 'further just orders' when a party 'fails to obey an order to provide or permit discovery.' Courts, however, have disagreed over whether these sanctions can be applied to Rule 26(c) protective orders, though the vast majority of courts have held that they can. The discrepancy largely stems from the debate over whether protective orders issued during discovery are discovery orders for purposes of Rule 37 . . . The Federal Rules of Civil Procedure expressly grant courts authority to issue sanctions in response to violations of 'order[s] to provide or permit discovery.' In addition to this explicit grant of authority, the inherent power of courts to sanction operates in the background, filling in gaps left by the Federal Rules under certain circumstances.")

67. For example, context alone may suffice to inform **ΠB** of **ΠA**'s breach. Should **Δ** solicit a meeting with **ΠB**, making pointed reference to **ΠB**'s open source offerings while casually referencing the fact that **ΠA** has brought action against **Δ**, **ΠB** would probably infer the existence of **ΠA**'s breach even without **Δ**'s explicit notification. In such a scenario, it would likely be extremely difficult to demonstrate that **Δ** violated a protective order as no discovery information (save **ΠB**'s identity, which is unlikely to have been explicitly covered by the order) was used.

68. Once **ΠB** has begun litigation, it is more likely that **ΠB** will be able to play **ΠA** and **Δ** off one another to acquire the highest purchase price capacity of the two.

from the preceding discussion (e.g., anticipate **Δ**'s purchasing price, hide or at least make ambivalent the value of $Cost_{A1}$ and $Benefit_{A1}$, etc.). Accordingly, this section instead briefly calls attention to proactive actions available to $\mathbf{\Pi^A}$, which may not be simply counterpoints to the above discussion.

A. Trade Secret-Contract Prevention

Where, as in *XimpleWare*, **Δ** had a preexisting relationship with $\mathbf{\Pi^A}$, $\mathbf{\Pi^A}$ may attempt to contractually deny **Δ** the ability to identify and act upon open source violations in $\mathbf{\Pi^A}$'s products. One should note that such a provision may require considerable foresight, indeed, more than is presently typically applied in such contracts. Particularly, existing provisions regularly *absolve* $\boldsymbol{\Pi^A}$ *of liability to* $\boldsymbol{\Delta}$ for such breaches, but *do not limit* $\boldsymbol{\Delta}$*'s disclosure options* concerning such liability.[69] This section considers a contractual provision specifically identifying the breach of an open source license as $\mathbf{\Pi^A}$'s trade secret, which **Δ** agrees to keep confidential.[70] While possibly doing much to limit **Δ**'s options, such a provision may still be subject to various limitations as outlined below.

1. Relevant Trade Secret Law

The author is not aware of any specific legal doctrine, which would prevent $\mathbf{\Pi^A}$ from characterizing $\mathbf{\Pi^A}$'s breach of an open source license as a trade secret. Indeed, such an act would appear to fall well within the "literal" definition of a trade secret in most jurisdictions. For example, in California a trade secret is defined as:

> "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: [¶] (1) **Derives independent economic value**, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and [¶] (2) Is the **subject of efforts that are reasonable under the circumstances to maintain its secrecy**." (§ 3426.1, subd. (d).)[71]

Breach of an open source license is certainly "information" from which $\mathbf{\Pi^A}$ "derives independent economic value" since it is unknown to other

69. Indeed, the Author has often seen the former, but never the latter.

70. As will be discussed in greater detail below, there are many ways to characterize this contractual provision. For example, rather than characterize an open source breach as a "trade secret" the drafter may include a provision indicating that $\mathbf{\Pi^A}$'s "service providers" and associated contractual relationships are trade secrets. The provision may deny **Δ** from contacting $\mathbf{\Pi^A}$. Broadly drafted, the latter provision may have as restrictive an effect as the former.

71. UTSA: CAL. CIV. CODE § 3426(1)(d).

persons (i.e., $\mathbf{\Pi^B}$) who could sue for damages ("economic value") from its "disclosure". The contract provision itself would certainly demonstrate that the "trade secret" was subject to "efforts . . . to maintain its secrecy".

Not only state, but federal law, would appear to support such a trade secret interpretation. The Defend Trade Secrets Act (DTSA) similarly defines a trade secret as:

> (3) the term "trade secret" means **all forms** and types of financial, **business**, scientific, technical, economic, or **engineering information**, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> (A) the owner thereof has taken **reasonable measures to keep such information secret**; and
>
> (B) the information **derives independent economic value**, actual or potential, from **not being generally known to, and not being readily ascertainable through proper means by, another person** who can obtain economic value from the disclosure or use of the information[72]

Again, the breach would likely qualify as "business . . . information" by this definition.

Under the DTSA, it may be possible for $\mathbf{\Delta}$ to disclose the noncompliance under a whistleblower exception, such as § 1833:

> §1833. Exceptions to prohibitions
>
> (a) In General.-This chapter does not prohibit or create a private right of action for
>
> (1) [. . .]; or
>
> (2) the disclosure of a trade secret in accordance with subsection (b).
>
> (b) Immunity From Liability for Confidential Disclosure of a Trade Secret to the Government or in a Court Filing.
>
> (1) Immunity.–An **individual** shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that-
>
> (A) is made-
>
> (i) in confidence to a Federal, State, or local government official, either directly or indirectly, **or to an attorney**; and

72. 18 U.S.C. § 1839(3) (emphasis added).

> (ii) solely for the purpose of reporting or investigating a **suspected violation of law**; or
>
> (B) **is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal**[73]

Although the statute does not define "individual", because the term "entity" is used separately it appears that "individual" refers only to human persons and not business entities. Despite this specificity, if the disclosure could be characterized as the action of an individual, rather than a breach of **Δ** as an entity, the provision may protect that individual from action by **Π^{A}**. This may simultaneously permit **Δ** the benefit of making good on its threat (assuming the individual does not appear as **Δ**'s agent). Particularly, there does not appear to be any reason to think that the disclosure may be made "to an attorney" under B(A)(i), would not include a disclosure to **Π^{B}**'s attorney.

However, the "violation of law" referred to in B(A)(ii) is not clearly a "breach of contract", but appears rather to refer to a breach of state or federal law.[74] This doesn't mean that B(A)(ii) won't provide the basis for the individual's disclosure, but it may be that **Δ** must find some other explicit federal or state law by which an individual may disclose to **Π^{B}**'s attorney. For example, "law" may be a state unfair competition statue, such as California Business and Professions Code 17200[75], while the federal unfair competition provision 15 U.S.C. 45 may suffice at the federal level.[76] While superficial and mostly speculative, this Section's brief assessment of trade secret law should help the reader to appreciate at least the *possibility* of characterizing the breach, or a related act, as falling within trade secret protection.

2. Doctrine of Unclean Hands and Exceptions

Even if **Π^{A}** successfully categorizes the breach as a trade secret, however, equity may prevent **Π^{A}** from enforcing the contractual provision. In California, for example, the doctrine of unclean hands can limit the enforcement of a contractual provision at odds with equity.

> The defense of unclean hands arises from the maxim, "'He who comes into Equity must come with clean hands.' " (Blain v. Doctor's Co. (1990) 222 Cal.App.3d 1048, 1059, 272 Cal.Rptr. 250 (Blain).) **The doctrine demands that**

73. 18 U.S.C. § 1833 (emphasis added).
74. 18 U.S.C. § 1833(b)(A)(ii).
75. California Business and Professions Code Section §§ 17200-17210 et seq.
76. 15 U.S.C. § 45 (2012).

> **a plaintiff act fairly in the matter for which he seeks a remedy. He must come into court with clean hands, and keep them clean, or he will be denied relief, regardless of the merits of his claim**. (Precision Co. v. Automotive Co. (1945) 324 U.S. 806, 814–815, 65 S.Ct. 993, 89 L.Ed. 1381; Hall v. Wright (9th Cir.1957) 240 F.2d 787, 794–795.) **The defense is available in legal as well as equitable actions**. (Fibreboard Paper Products Corp. v. East Bay Union of Machinists (1964) 227 Cal.App.2d 675, 728, 39 Cal.Rptr. 64 (Fibreboard); Burton v. Sosinsky (1988) 203 Cal.App.3d 562, 574, 250 Cal.Rptr. 33.) Whether the doctrine of unclean hands applies is a question of fact. (CrossTalk Productions, Inc. v. Jacobson (1998) 65 Cal.App.4th 631, 639, 76 Cal.Rptr.2d 615.) The unclean hands doctrine protects judicial integrity and promotes justice. It protects judicial integrity because allowing a plaintiff with unclean hands to recover in an action creates doubts as to the justice provided by the judicial system. Thus, precluding recovery to the unclean plaintiff . . .[77]

Because the breach of an open source contract is unlike the competitive advantage afforded by most trade secrets, in that it imposes on the legal rights of the open source licensor, a court may be more willing to apply unclean hands to the provision's enforcement. The court will need to balance the public policy aspects of such a provision alongside the parties' right to contract. Certainly, making confidential the harm caused by an FDA violation, or by illegal activity, would be unconscionable. But can failure to comply with an open source license be considered sufficiently egregious to obviate the parties' right to contract?

The answer to this question may depend upon the nature of the contractual provision's language. For example, open source compliance is fraught with difficulties regarding upstream licensees, authentic representations of upstream license terms, and other complications. In one pathological scenario, an upstream licensor may deliberately, or accidentally, misrepresent their right to license a piece of software. For example, a disgruntled software programmer may release her employer's proprietary code under the permissive MIT license. A downstream licensee may have no way of knowing of the upstream distributor's misrepresentation. With regard to the abstraction of Figure 2, the diagram would be modified as follows:

77. Kendall-Jackson Winery, Ltd. v. Superior Court, 76 Cal.App.4th 970, 973 (Cal. App. Ct. 1999), *as modified on denial of reh'g* (Jan. 3, 2000) (emphasis added) (internal citations omitted).

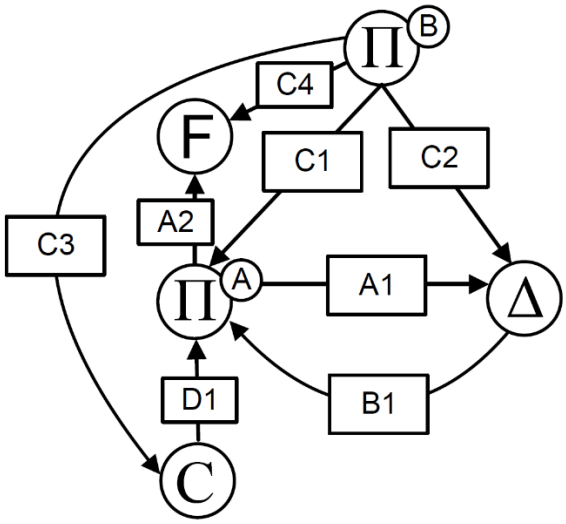

FIGURE 6: Generalized Litigation Topology with Fraudulent Contributor/Distributor

Here, a fraudulent distributor **F** is someone who purports to have the capacity to distribute code under an open source license, when in fact only the true owner $\mathbf{\Pi^B}$ has that right and has not authorized such a distribution. In this situation, $\mathbf{\Pi^A}$ is "as much a victim" as **C** and **Δ**, and indeed, the primary causes of action will be **A2** and **C4** against **F**. Where $\mathbf{\Pi^A}$'s contractual provision with **Δ** anticipates this scenario, particularly where it only asks that $\mathbf{\Pi^A}$ be given a chance to remediate before **Δ** discloses, it seems unlikely that **Δ** will succeed in a defense of unclean hands.[78] $\mathbf{\Pi^A}$'s motive is no longer clearly directed to the suppression of a deliberate violation. Rather, the contractual provision now appears to merely be a precaution against upstream bad actors, albeit a precaution that imposes some confidentiality restrictions on **Δ**. A prescient **Δ** will demand that the contract language be narrowly tailored to a situation involving only an **F** and exclude other violations by $\mathbf{\Pi^A}$, but such an "aggressive" stance would be unusual in most contractual negotiations.[79]

78. Such language directly anticipates, and to a certain extent, refutes the equitable basis for the defense of unclean hands. In this manner, $\mathbf{\Pi^B}$ would generally use language in the contractual provision directed to motives *other than* denying **Δ** access to $\mathbf{\Pi^B}$, which have the incidental effect of denying **Δ** access to $\mathbf{\Pi^B}$.

79. The temper of such a request would often disrupt otherwise "friendly" business negotiations.

B. Preemptive Due-Diligence

It hardly needs stating that the simplest way for $\mathbf{\Pi^A}$ to nullify the above discussion is simply not to violate any open source agreements. Such a factual situation obviates the entirety of the above tactic. Unfortunately, compliance is often a nontrivial task, particularly where a product incorporates many different open source components. A proactive $\mathbf{\Pi^A}$ should impose ongoing compliance reviews and developer education to mitigate breach opportunities. Waiting until a product's release to perform diligence may be imprudent, as this will require great time and cost to remediate any previously introduced violation. Similarly, waiting to perform diligence until preparing to bring **A1** may be too late to effectively remediate (indeed, the engineers now aware of the failure may be deposed and inadvertently disclose the existence of a defect). Thus, an ounce of early prevention may well be worth many pounds of cure.

CONCLUSION

This Article has sought to illuminate aspects of the litigation tactics that may arise when a defendant discovers an open source violation on the part of the plaintiff. As a bargaining tool, such knowledge can be incredibly value, but only under the particular factual circumstances regarding the character of the license, the interests of the copyright owner, and the nature of the plaintiff's business. Both parties have recourse to various defenses, but proactive due diligence is likely the most reliable method for nullifying the tactic's applicability.