

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month



Discovery of Source Code—Fashioning a Protective Order

Scenario

A technology company is involved in patent litigation that will require the production of source code. The general counsel wants a protective order that will protect the source code to the maximum extent possible.

Production of Source Code

In patent, trade secret and copyright litigation where computer-related software is accused or otherwise relevant, the parties must engage in the discovery of source code. Source code is the set of instructions for how a computer program operates, written in human-readable language. Source code is typically complex, very lengthy (sometimes reaching several million lines of programming), and requires expert review, analysis and explanation. Companies whose software is integral to their products and services protect their source code zealously, considering it to be among their most confidential information. As a result, they will not make it available for discovery without the entry of a suitable protective order.

In December 2015, the Sedona Conference, a nonprofit research and educational institute whose mission is to study and advance law and policy regarding electronic discovery, intellectual property rights, antitrust law and complex litigation, published a “Commentary on Patent Litigation Best Practices: Case Management Issues from the Judicial Perspective Chapter.” Best Practice 19 in this Commentary focuses on the discovery of source code. It states: “The court should require the parties to address in the Rule 26 joint discovery plan how and where they believe any computer source code production should be made available to the parties and experts.” The Commentary suggests that discovery in patent litigation cannot begin in earnest until there is a protective order regarding how, when and where source code will be produced. As a result, the Sedona Conference recommends that the court require that before the first case management and scheduling conference, the parties should set forth in their Rule 26 joint discovery plan exactly how and where they believe any source code should be produced. This way the court can resolve issues before any undue delay or expense is incurred.

Because source code is guarded so closely, the producing party typically provides it for inspection rather than producing copies of the source code. Typically, only outside counsel for the inspecting party and pre-approved experts can inspect code. Further, inspection typically takes place on a stand-alone (i.e., non-networked) computer.

Protective Order Issues

When preparing a protective order governing the production of source code, areas of consideration include the following:

- *Use of analytic tools.* A source code expert will typically need to use analytic/forensic tools to search the source code (e.g., Grep). To avoid disputes, the protective order should address whether this is permitted and, if so, which tools are permitted. The inspecting party may further wish to specify that such tools be loaded onto the review computer before inspection begins.
- *Place.* Inspection typically occurs at the offices of the producing party's litigation counsel. However, some parties insist that inspection take place at a certified escrow facility (e.g., Iron Mountain). If inspection is to take place at an escrow facility, the protective order should specify who will cover the escrow fees.
- *Timing.* Source code inspection is typically conducted during the producing party's counsel's normal operating hours and after a specified minimum amount of notice.
- *Copying.* Some producing parties insist that the access ports and other functionality on the inspection computer be disabled in order to prevent unauthorized copying. Inspecting personnel may also be prohibited from bringing memory devices into the inspection room. Further, some protective orders specify how notes may be recorded.
- *Printing.* There are invariably restrictions on the overall amount of source code that can be printed. These restrictions are typically based on the quantity of pages and the overall proportion of source code. A carefully written protective order also specifies that review of the source code in the first instance is to occur via the stand-alone computer, rather than by printing out the code en masse. The inspecting party may wish to specify that it will have access to the printed pages at the same time it is inspecting the electronic code.
- *Experts.* The producing party typically requires that the inspecting party's expert(s) be pre-approved by the producing party after the inspecting party has produced information sufficient to allow the producing party to determine whether the potential expert has a potential conflict. There are usually presumptive limitations on the number of experts allowed to inspect the source code.
- *Production.* Once the source code is printed, the producing party is typically given a few days to produce the printed copies to the inspecting party. The printed pages are often endorsed with a special source code designation defined in the protective order.
- *Review and access to printed production.* The inspecting party is generally prohibited from keeping an electronic copy of the source code and may be required to log access to the printed copies. Provisions should be made so that a copy can be delivered to the inspecting party's expert for further review, and for court filings. Further, the parties may wish to specify who may be shown the printed production at deposition, and whether the source code may be disclosed to mock juries.
- *Prosecution bar.* Protective orders in patent cases invariably contain a "prosecution bar," which forbids the attorneys who review the code from prosecuting patent applications related to the technology at issue for a specified amount of time. For further guidance, see the Sedona Conference Commentary on Patent Litigation Best Practices: Case Management Issues from the Judicial Perspective Chapter, Best Practice 20.
- *Unauthorized disclosure.* The protective order should address what steps must be taken should there be an unauthorized disclosure.

Note that some courts have developed model protective orders that govern discovery until a specifically tailored protective order can be entered. See N.D. Cal., Stipulated Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets (2014), available at <http://www.cand.uscourts.gov/model-protective-orders>.

Conclusion

Protective orders relating to the production of source code frequently contain specific provisions not necessarily found in many protective orders. It can be most efficient for the parties to negotiate the protective order prior to the initial case management conference, so they can present any disputes to the court at that time. To avoid disputes over an entered protective order, consider a protective order that is as specific as reasonably possible.

For inquiries related to this Tip of the Month, please contact Kim Leffert at kleffert@mayerbrown.com or Graham Buccigross at gbuccigross@mayerbrown.com.

To learn more about Mayer Brown's [Electronic Discovery & Information Governance](#) practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, Ethan Hastert at ehastert@mayerbrown.com, or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.