

Vendor Truth Serum



Greg Klass, Georgetown Law Center and Eric Burger, Georgetown Department of Computer Science https://s2erc.georgetown.edu/projects/vendortruthserum

- Problem: The DeWitt Clause
- You shall not . . . (e) Perform, publish, or release to any third parties any benchmarks or other comparisons regarding the Software or User Documentation.
- Scenario: DHS SWAMP wanted to let users know S.E. tools' coverage, so users could chose combination of tools to fully test software
- DeWitt Clauses prevented DHS from doing that
- Research: How can private or public (e.g., NIST, DHS, NSA) entities share results?
- Research analyzed contracts, contract law,
 FARs, and case law
- Result: A contract is a contract, even if it is a bad contract
- Bright Spot: Microsoft contract

You may disclose the results of any benchmark test of the .NET Component, provided that ...:

(1) you must disclose all the information necessary for replication of the tests, ...;

(2) you must disclose the date(s) that you conducted the benchmark tests, along with specific version information for all Microsoft software products tested ...;

(3) your benchmark testing was performed using all performance tuning and best practice guidance ...;

(4) it shall be sufficient if you make the disclosures provided for above at a publicly available location such as a Web site ...



- Solution for consumers: *Consumer Review Fairness Act* (PL 114-258, December 2016):
- \$2(a)(2) COVERED COMMUNICATION. The term "covered communication" means a written, oral, or pictorial review, performance assessment of, or other similar analysis of, including by electronic means, the goods, services, or conduct of a person by an individual who is party to a form contract with respect to which such person is also a party.
- \$2(b)(1) IN GENERAL. Except as provided in paragraphs (2) and (3), a provision of a form contract is void from the inception of such contract if such provision—
 - (A) prohibits or restricts the ability of an individual who is a party to the form contract to engage in a covered communication;

- Impact:
- DeWitt Clauses affect more than just software
 - Supply chain
 - Physical, human harm resulting from undetected software errors (CPS)
- Next research steps
- Collect attributable cases
 where failure of
 information sharing caused
 harm
- This is our ask for you

- Next policy steps
- Private/Public entities:
 Develop model legislation
 similar to PL 114-258
- Public entities: Update
 FARs to prohibit clause

This material is based upon work supported by the National Science Foundation under Grant No. 1362046 and the industry affiliates of the Security and Software Engineering Research Center (S²ERC). The views and analysis provided are entirely our own and not attributable to any other party. Support for this work included support from the Department of Homeland Security Science and Technology Directorate. Payments are made to Georgetown University and the funds are used to cover the expenses of the study and related academic and research activities of the institution.

