

The FTC's Flawed Data Security Enforcement Program and Suggestions for Reform (FTC hearings, Comment 8)

May 31, 2019

[Geoffrey A. Manne](#), [Gus Hurwitz](#), [Julian Morris](#), [Kristian Stout](#) and [Dirk Auer](#)

Comments of the International Center for Law & Economics:

Several pressing issues are raised by the ongoing need for data security as underscored by high profile breaches. One of the core problems in this area, however, is not simply that firms have inadequate data security, but that lawmakers have, to date, broadly failed to offer a viable standard by which firms can guide their conduct in this area.

The flawed strategy which the FTC currently deploys to deal with data security issues is a prime example. In brief, the Commission's over-reliance on enforcement by consent decrees has created a quasi-regulatory approach to data security, eschewed the fundamentally useful aspects of a true common law approach to developing liability rules, and as a consequence provided little record of what actually amounts to liability for "unreasonable" data security. A true standard would include such components as: the assessment of reasonable care on the part of the tortfeasor, the thorough analysis of causality, an economically grounded computation of harm, and the establishment that harm is likely absent some level of care.

Given these failings, the FTC should consider implementing reforms that might bring its decisional practice closer to the common law tradition. These include giving more weight to economic analysis (notably by allowing the FTC's Bureau of Economics to play a greater role in data security proceedings), adopting modest measures that would increase the transparency of the FTC's data security decisions (thereby increasing legal predictability), bringing greater judicial review to data security proceedings, and incentivizing firms to better communicate their data security activities.

[Click here to read full comments.](#)

[View Article](#)