

QVC Showed No Damages from Resultly's Web Crawler Slowdown

QVC, Inc. is not entitled to an injunction against a small start-up that sent web crawlers to the online retailer giant, overloading QVC's servers for two days and impairing consumers' ability to use the site.

QVC alleged that Resultly, Inc. violated the Computer Fraud and Abuse Act (CFAA) because it sent bots to gain pricing information from QVC's site, which slowed down QVC's server. The bots were looking for information to list QVC's items on Resultly's site, where the items could be sold and earn a commission for Resultly.

A U.S. District Court judge in Pennsylvania found that QVC failed to show the likelihood of success on the merits required for a preliminary injunction. The court said QVC did not satisfy the CFAA's requirement that, "when Resultly crawled QVC's website, it intended to cause damage to QVC's server." In fact, the judge found, "Resultly had no incentive or desire to cause QVC's webpage to slow down, let alone overload. To the contrary, Resultly's business plan requires that the websites it crawls stay functional."

The court said there was "compelling and credible testimony that it would have been antithetical to Resultly's business goals to render QVC's server unavailable to customers. As a growing start-up, Resultly was attempting to form positive business relationships with the retailers whose websites it crawled, not alienate them." The testimony also showed that Resultly stopped sending bots to the QVC site in response to QVC's request.

Resultly uses a computer code to crawl the web to search public websites of online retailers so it can advertise their merchandise on its own site. If consumers subsequently buy the product, Resultly receives a commission on the sale. Resultly uses an open source program to control its bots.

QVC sought to stop Resultly from crawling on its website and also sought to stop Resultly from selling its computer program to others. The section of the CFAA under which QVC filed its claim, requires QVC to show that Resultly "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization to a protected computer."

The trial court found that Resultly did not intentionally cause damage. To the extent that QVC's servers slowed down, the court said it was caused by the failure of Resultly "to iron out certain wrinkles in its operations. While Resultly's conduct may be sufficient to demonstrate negligence or recklessness, the Court cannot infer that Resultly intended to cause damage to QVC's servers," as required by the CFAA.

The court noted that Resultly may be in precarious financial condition, but that is not a sufficient basis to enjoin the company from selling its web crawler program, which is based on open source software, “which means it is in the public domain on the Internet.” The court said the evidence shows that QVC has the “undisputed ability to protect itself against any future outages caused by unknown bots.”

QVC, Inc. v. Resultly, LLC, E.D. Penn., No. 14-6714, filed March 13, 2015.

Balough Law Offices, LLC, is a Chicago-based law firm which focuses on cyberspace, internet, and business law. Our homepage is balough.com.