

Curbing Domain Name Registration Abuse: A Legal Framework in the Implementation of the Anti-Cybersquatting provision of the Cybercrime Prevention Act of 2012

Ferdinand M. Negre

Gonzalo D.V. Go III

57 ATENELO L.J. 949 (2013)

SUBJECT(S): INTELLECTUAL PROPERTY, CRIMINAL LAW, CYBERCRIME, CONSTITUTIONAL LAW

KEYWORD(S): CYBERSQUATTING, CYBERCRIME PREVENTION ACT OF 2012, TRADEMARKS, BAD FAITH

The recently enacted Cybercrime Prevention Act of 2012 has drawn much controversy for many reasons, one of which is the fact that it introduces new “crimes” so to speak, in our legal system, crimes which, given the multitude of users on the internet, any of us could commit it. One such crime is called cybersquatting, and it is this offense that is the topic of this Article.

Cybersquatting is the act of registering a domain name using a trademark, personal name, or other commonly known mark of another person or entity, in order to achieve some illegal purpose. These purposes may range from benefitting one’s self through the extortion of a high bid price for the domain name, to harming the rightful owner of the domain name by using the website to tarnish the good will and reputation associated with the trademark used. It is this evil which the anti-cybersquatting provision seeks to suppress. In this Article, the Authors discuss the provision and the relevant information about the addressing system of the internet with which it works, in detail. They also tackle possible constitutional objections to the provision, as well as its justification as a valid exercise of the legislature’s police power. Finally, the Article is also replete with examples of intellectual property cases from the World Intellectual Property Office Arbitration and Mediation Center, which shed more light on the applicability and importance of an anti-cybersquatting provision in any legal system which exists amidst a population of which a huge percentage are constantly using the internet.