

2014 - 2015 Legislation Review - I.P. and Computer Laws
by Robert Kain

**A. SLAPP: Florida Statute 768.295:
Strategic Lawsuits Against Public Participation (SLAPP lawsuits)**

The SLAPP statute relates to free speech which is defined as public issues which covers any written or oral statement that is protectable under the law. The statute provides that any person (or governmental entity) may not file a lawsuit “without merit and primarily because such person or entity has exercised the constitutional right of free speech in connection with a public issue...,” such as First Amendment speech. The defendant may seek an order dismissing the action or file a motion for summary judgment. After the claimant files a response, the statute states “as soon as practicable, the court shall set a hearing on the motion which shall be held at the earliest possible time after filing of the claimant’s... response.” The statute provides for attorneys fees for the prevailing party.

B. The Patent Troll Prevention Act- Florida Statute 501.991

The Troll Act regulates the sending of patent infringement demand letters and the filing of lawsuits and prohibits bad-faith assertions of patent infringement. The Troll Act requires that demand letters include a patent number, name and address of the patent owner, and factual allegations regarding the target’s products which are covered by the claims of the patent. In order to determine what is a “bad-faith assertion,” the party charging infringement must, before sending the demand letter, “conduct an analysis comparing the claims in the patent to the target’s products.” Further indicia of bad faith is found when the demand letter lacks the required information (patent number, name and address of patent owner), requests payment of a license fee, when the license is not based on a reasonable estimate of the patent value, if the person knew the patent was unenforceable, or if the claim of patent infringement is deceptive. Previously filed or threatened lawsuits also provide indicia of bad faith.

The statute also provides that a person “has not made a bad-faith assertion” when the demand letter contains the aforementioned information, or when the person asserting the patent provides the required information when the target-accused infringer requests such data, when the patent owner engages in a good-faith effort to establish that the target infringed, when the patent plaintiff made a substantial investment in the patented invention, when the patent plaintiff is the inventor or assignee of the original inventor, or if the person has demonstrated good faith business practices or has successfully enforced the patent in the past.

If a lawsuit is initiated, the defendant may move the court for determination that a bad-faith assertion of patent infringement has been made and may seek a protective order. If bad-faith is established, “the court **must require** the plaintiff to post a bond in an amount equal to the lesser of \$250,000 or a good-faith estimate of the target’s expense of litigation.” The statute provides for a private cause of action and indicates that such bad faith assertion is an act of unfair

or deceptive trade practice. In the private right of action, the prevailing party is entitled to reasonable attorneys fees. The troll statute exempts actions by institutions of higher education or relief sought under 35 U.S.C. 271(e)(2).

C. Digital Goods Act - Florida Statute 501.155 entitled “True Origin of Digital Goods Act.”

The Digital Goods Act excludes from its coverage interactive computer services and communications services. It relates to commercial recording or audiovisual works which means a recording or audiovisual work “but does not include an excerpt consisting of less than substantially all of the recording or audio visual work.” The Digital Goods Act requires that the owner of the website disclose certain information if that website deals “in substantial part in the electronic dissemination of third-party commercial recordings.” In that event, the website owner or operator shall “clearly and conspicuously disclose his or her true correct name, physical address, telephone number or email address.” This information may be posted on the homepage, the “about us” webpage, the “contact us” webpage, or other conspicuous place. Injunctive relief is provided for but, as a condition precedent, “the grieved party must make reasonable efforts to place an individual alleged to be in violation of this section on notice that the individual may be in violation...”. The prevailing party is entitled to attorneys fees.

D. The Computer Abuse and Data Recovery Act, Fla.Stat. §668.801 (“CADRA”) (effective October 1, 2015).

CADRA establishes a new civil action against unauthorized persons, such as computer hackers, who damage business computers or online data storage systems which contain business information. CADRA is limited to business computer hardware and business information stored in computers or online, in the cloud, on the Internet. If a hacker or a terminated employee takes data and causes damage, the business owner can sue under CADRA and recover damages and obtain injunctive relief.

The data or software must “protected” under CADRA with a password, access control, security system, key fob or lock, biometric identifier (fingerprint, retina scan), or other technological access device (a “TAB”)(defined as “protected” computers and data).

The CADRA actor must: “knowingly and with intent to cause harm or loss: (1) obtain[] information from protected computer without authorization and, as a result, causes harm or loss; (2) cause[] the transmission of a program, code or command to a protected computer without authorization and causes harm or loss; or (3) traffic[] in any technological access barrier through which access to a protected computer may be obtained without authorization”. Liability is based upon harm and loss to the business owner.

CADRA specifies “authorized users” as users such as a “director, officer, employee, third party agent, contractor, or consultant of the owner [a “DOE3”] ... [who] is given express

permission by the owner ... to access the protected computer” through a TAB. DOE3s are not authorized if they are “terminated” by the owner or “upon cessation of employment, affiliation or agency.” An act “without authorization” is one where the actor: (a) is not an authorized user; (b) steals a TAB; or (c) “circumvent[s] a technological access barrier [TAB] on a protected computer without the express or implied permission of the owner.” Some passwords are not effective controls (“1234,” “password,” and “admin”). Therefore, a CADRA “without authorization” TAB circumvention “does not include circumventing a technological measure that does not effectively control access to the protected computer or the information stored in the protected computer.”

As for remedies, the business owner can recover: actual damages, lost profits, economic damages, violator’s profits, loss due to impairment of the data-code, harm due to denial of access, damage assessment fees, remediation costs, and damages for interruption of SAAS service. An injunction permits recovery of originals and all copies of the data - program. Attorneys fees are available to the prevailing party.

In the past, practitioners employed the Florida Computer Crimes Act, Fla. Stat. § 815.01 and the Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (“CFAA”). These are criminal statutes with a civil remedy. The scope of the CFAA has been called into question by several contradictory appellate court cases primarily over the meaning of “authorized access.” Florida’s Computer Crimes Act is not effective because a civil action can only be brought after a conviction by the State.

E. Drone Surveillance Act: Florida Statute 934.50, title: “Freedom from Unwarranted Surveillance Act.”

This act governs surveillance by a drone of privately owned real property and the observation of persons “with sufficient visual clarity to be able to obtain information about their identity, habits, conduct, movements, or whereabouts.” The use of drones is prohibited to record an image of privately owned real property of the owner or “in violation of such person’s reasonable expectation of privacy without his or her written consent.”

Exemptions are provided if a person or entity is engaged in business or profession licensed by the state and “if the drone is used only to perform reasonable tasks within the scope of practice are activities permitted under such person’s or entity’s license.” Specifically excluded are employees or contractors of a property appraiser, utility companies, and aerial mapping if used in compliance with FAA regulations.

Remedies for violations include a civil action for violation of the drone surveillance act and injunctive relief. A prevailing party is entitled to reasonable attorneys fees.

Robert Kain
Board Certified I.P. Specialist
Kain Spielman , P.A.
Fort Lauderdale, FL.
ComplexIP.com 954-768-9008