McAfee & Taft

TIP SHEET™

an informational newsletter on intellectual property matters

JULY 2012

IN THIS ISSUE

INTELLECTUAL PROPERTY PRACTICE GROUP

Mike LaBrie, *Group Leader*
michael.labrie@mcafeetaft.com
(405) 552-2305

Rachel Blue
rachel.blue@mcafeetaft.com
(918) 574-3007

John Burkhardt
john.burkhardt@mcafeetaft.com
(918) 574-3001

Ryan Cross
ryan.cross@mcafeetaft.com
(405) 270-6026

Bob Dace
bob.dace@mcafeetaft.com
(405) 552-2268

Brad Donnell
brad.donnell@mcafeetaft.com
(405) 552-2308

Cliff Dougherty
cliff.dougherty@mcafeetaft.com
(405) 552-2302

Matt Gibson
matt.gibson@mcafeetaft.com
(405) 552-2348

Bill Hall
bill.hall@mcafeetaft.com
(405) 552-2218

John Kenney
john.kenney@mcafeetaft.com
(405) 552-2244

Sasha Legere
sasha.legere@mcafeetaft.com
(405) 270-6011

Seller beware: In-app purchases by minors may constitute unique, voidable contracts

BY JESSICA JOHN BOWMAN
jessica.johnbowman@mcafeetaft.com

When an app is purchased, a contractual relationship is created between the company selling the app and the user, even when the app is "sold" for free. But does that mean that the company selling the app also creates contractual relationships with those who subsequently use the app? According to a recent opinion by the U.S. District Court for the Northern District of California, the answer may be yes.

The case before the California court, styled *In re Apple In-app Products Litigation*, concerned Apple's relationship with individuals who made "in-app" purchases. An in-app purchase means a purchase opportunity offered and authorized within an application (usually a game). The application provides the user with the option of authorizing the purchase of virtual items—such as Smurfberries that can be used as currency in the popular Smurfs' Village game—for use within the app.

Ordinarily, to purchase an app or in-app product through Apple, a user must provide his iTunes account information, a password, and a valid credit card number. Until recently, however, a second password entry was not required for app or in-app purchases made within 15 minutes of the most recent password entry. As a result, users could make in-app purchases without the knowledge, consent, or authorization of the iTunes accountholder being charged for the purchase.

The plaintiffs in *In re Apple* were parents whose children had purchased thousands of dollars of in-app products without the parents' knowledge during the 15-minute window during which their iTunes accounts remained "active" after a password entry. The plaintiffs argued that, by selling first the app and then the related in-app products, Apple had in essence entered into a series of separate app-related contracts, which are voidable at the option of the minors who agreed to the sale.

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

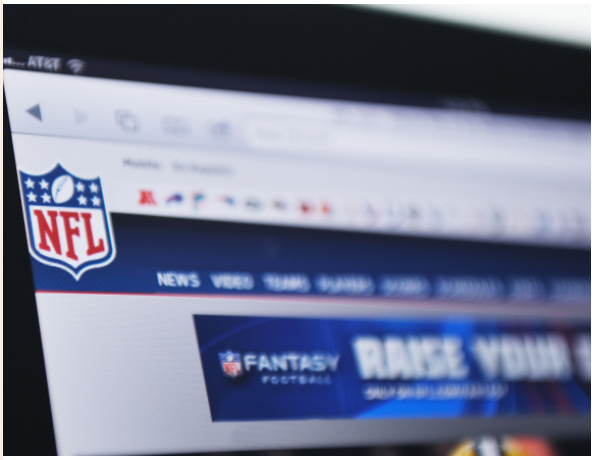
The question at the heart of this lawsuit is, do the terms and conditions governing the initial purchase of the app cover all subsequent sales within the app, or are in-app purchases independent sales contracts? For the time being, the court has permitted the parents to proceed on their separate-contract theory. If the court ultimately concludes that separate contracts existed between Apple and the minor purchasers, Apple could face a significant financial loss, as the minor purchasers will have unique contractual defenses and remedies unavailable to their adult parents.

This case could have serious implications for companies that develop and sell apps with built-in future-purchase opportunities. App developers should carefully consider the way in-app purchases are presented to the user, and the manner in which a user may agree to a purchase, particularly where apps are designed for use by minors. For example:

- Consider the price of the in-app purchase, and the relative appeal that the item would have to a minor child.
- Evaluate when, during the course of the game, an app will prompt a decision with monetary impact: Is it easy for the child to reach that point? Is the purchase presented as the only means of continuing the game without restarting?
- Avoid exhortative language like "buy this now" or "only 2 left" if the app is created to appeal to children.
- Create in-app parental controls, notify purchasers of in-app purchase opportunities at the time the app is initially downloaded, and remind parents that they may prevent unauthorized purchases by utilizing "airplane mode" on their mobile devices.

By taking care to clearly define the contractual relationship and build in procedural safeguards prior to each transaction, a company may protect itself from future claims that in-app purchases are voidable or invalid based on the identity of the user.

Internet expansion to create opportunities, concerns for brand owners



BY RYAN LOBATO

The Internet is expanding again, creating new concerns for trademark owners. In addition to the 22 presently existing generic top-level domains (e.g., .com, .org, .edu, etc.), the naming authority for the Internet, ICANN, has decided to permit applicants to specify their own top-level domain names.

On June 13, 2012, ICANN published the list of applicants and the prospective domain names. While some companies utilized a .[brand] naming strategy, including the American Automobile Association (.AAA), the National Football League (.NFL), and Nike, Inc. (.NIKE), other applicants have selected generic words, including (.CHURCH), (.SPORTS), and (.NEWS). Once finally approved, any or all of these generic top-level domains (gTLDs) may be in use as early as March of 2013. Although the application window is now closed, more

CONTINUED ON NEXT PAGE

INTELLECTUAL PROPERTY PRACTICE GROUP (CONT.)

Ryan Lobato
ryan.lobato@mcafeetaft.com
(405) 552-2390

Mike McClintock
michael.mcclintock@mcafeetaft.com
(405) 552-2213

Jim McMillin
james.mcmillin@mcafeetaft.com
(405) 552-2280

Andy Peterson
andy.peterson@mcafeetaft.com
(405) 552-2333

Tony Rahhal
anthony.rahhal@mcafeetaft.com
(405) 552-2306

Reid Robison
reid.robison@mcafeetaft.com
(405) 552-2260

Jay Shanker
jay.shanker@mcafeetaft.com
(405) 552-2385

CONTINUED FROM PREVIOUS PAGE

than 1,900 applicants paid the non-refundable $185,000 application fee to take advantage of the prospect of choosing a new Internet gTLD.

Trademark owners should be on alert for brand opportunities and risks. For example, the gTLD (.GAMES) is likely to issue. By way of example, the domain HUNGER.GAMES may be of particular interest to the rights owners of the currently popular movie of the same title.

We encourage brand owners to review the list of gTLDs involving marketing, sales, information systems administration and trademark counsel perspectives. Many of the new gTLD owners are likely to open their gTLDs to the public. An early application and monitoring strategy will help brand owners secure desired domains and prevent the more problematic uses. If a domain name problem arises under a new gTLD, various dispute resolution mechanisms have been set forth by ICANN. Please feel free to contact us to obtain more information.

» The list of applicants for new gTLDs may be **reviewed at the ICANN website**

When cyber-threat protection and privacy concerns collide

BY RYAN LOBATO

The Cyber Intelligence Sharing and Protection Act ("CISPA") is a pending legislative proposal aimed at protecting against cyber-threats and cyber-attacks. CISPA follows the much publicized and now effectively defunct legislative proposals Stop Online Piracy Act ("SOPA") and the Protect IP Act ("PIPA") as a means to combat online misconduct. On January 18, 2012, Internet megasites Wikipedia, Craigslist, Reddit, Mozilla, Linux and others voluntarily shut down their websites to protest the passage of SOPA and PIPA. Following these protests, SOPA and PIPA were indefinitely postponed. Although some critics see CISPA as a new SOPA/PIPA, CISPA has a somewhat different aim and has received much less protest from the online community.

While not required to do so, CISPA permits certain technology and manufacturing companies to share users' personal information with the U.S. government, including information presently protected by privacy laws such as HIPAA (Health Insurance Portability and Accountability Act), VPPA (Video Privacy Protection Act) or FERPA (Family Education Rights and Privacy Act), without disclosing to the users that their information has been shared. Consequently, otherwise private information, including video rental records, book rentals, newspaper subscriptions, online reading or data protected by state consumer protection laws (like utility usage records) may freely be shared under CISPA despite existing privacy rules and sharing safeguards.

CISPA supporters state that the availability of this information will help the government identify cyber-threats and prevent cyber-attacks. Critics state that this is an unnecessary violation of privacy rights, accomplishing no more for the private sector than the currently enacted Wiretap Act and Electronic Communications Privacy Act and allowing the U.S. government unfettered access to private information for which it would otherwise require a warrant.

CISPA was passed by the U.S. House of Representatives by a vote of 248 to 168 on April 26, 2012. While by no means a foregone conclusion, pundits presently speculate that CISPA will not make it onto the Senate's agenda. Two alternative bills generally aimed at the same measures, the Cybersecurity Act of 2012 ("CSA") and the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology ("SECURE IT"), are likely to be taken up instead.

We will keep you informed of these and other developments as they progress.

McAfee & Taft
ATTORNEYS & COUNSELORS

OKLAHOMA CITY
TWO LEADERSHIP SQUARE
TENTH FLOOR
211 N. ROBINSON
OKLAHOMA CITY, OK 73102
405.235.9621

TULSA
1717 S. BOULDER
SUITE 900
TULSA, OK 74119
918.587.0000

www.mcafeetaft.com