Employers increasingly are suing former employees who have left to join or form competing companies using the civil remedies available under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C.A. § 1030. They use the CFAA to prevent their former employees from using sensitive information obtained from the former employer’s computer system. The scope of the CFAA, however, is subject to hot debate among the federal courts, as highlighted by a recent case from the District of Minnesota.

In Walsh Bishop Associates, Inc. v. O’Brien, Civil Action No. 11-2673 (DSD/ AJB), 2012 WL 669069 (D. Minn. Feb. 28, 2012), the court interpreted a provision of the CFAA, 18 U.S.C.A. § 1030(a)(2)(C), which subjects an individual who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer” to civil liability should the plaintiff meet certain conditions. In particular, the court had to determine the scope of the phrase “exceeds authorized access,” which the CFAA defines as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.” 18 U.S.C.A. § 1030(e)(6). The plaintiff argued that a person exceeds authorized access by accessing information in order to use it in a manner contrary to an employer’s interests and use policies. The O’Brien court, however concluded, among other things, that subsection (a)(2) is not based on use of information, but rather access to information. Plaintiff’s interpretation therefore
Table of CONTENTS

New Case Highlights Split of Authority Interpreting the Computer Fraud and Abuse Act
By Brian P. Bialas .......................................................... 1

From the EDITOR
By Michael D. Scott ..................................................... 3

Legal Process Outsourcing: A Cost-saving Scheme Which Might End Up Costing More
By Victor Lau & Vanja Bulat ........................................ 4

Defending Your Brand in the .xxx World
Bry Anthony V. Lupo & Amy E. Salomon ........................ 5

Will the Pinterest “Nopin” Tag Put Online Image Owners on the Defensive on Implied Copyright Licenses? Should We Look to Robots.txt as Precedent?
By Jeff Neuburger ........................................................ 6

Germany: E-commerce Obligations—Order Buttons Need to be Changed
By Dr. Fabian Niemann & Stefan Kujat .......................... 8

NTIA Requests Comments on the Development of Consumer Data Privacy Codes of Conduct
By Stephanie M. Phillips, William E. Cook, Jr. & Michael Levin .................................................. 8

FTC
FTC Gets Court Order Shutting Down Pyramid Scam ................. 10
FTC Approves Safe Harbor Program under COPPA for Aristotle International, Inc. .................... 11
FTC Stops Deceptive Practices of Marketer Who Used Bogus ‘Free’ Trial Offers ................................ 12

Videogame Law
By Davis LLP Videogame Law Group ............................... 13

EA denied SSX.com
(Submitted by Tania Da Silva) ......................................... 13

EA lawsuit - further thoughts
(Submitted by David Spratley) ...................................... 13

Fallout from Bethesda-Interplay lawsuit dissipates
(Submitted by David Spratley) ...................................... 14

Calendar of Events ................................................................ 15

Editorial Board

EDITOR-IN-CHIEF:
MICHAEL D. SCOTT,
Professor of Law
Southwestern School of Law

BOARD OF EDITORS:
MARCIA ADAMS
Corporate Counsel, Hewlett-Packard Co.
Palo Alto, CA

JAN C. BALLON
Greenberg Traurig
Silicon Valley, CA

HENRY BECK
Heller Ehrman White & McAuliffe LLP
New York, NY

THOMAS J. D’AMICO
Dickstein Shapiro Morin & Oshinsky LLP,
Chicago, IL

GEORGES C. FISCHER
Fischer & Forster
Sao Paulo, Brazil

PETER FRAZZA
Budd Larner Gross Rosenbaum Greenberg & Sade,
Short Hills, NJ

MARC S. FRIEDMAN
Silis Cammis Epstein & Gross P.C.
Newark, NJ

ERIC GOLDMAN
Assistant Professor, Academic Dir., High Tech Law Institute
Santa Clara University School of Law
Santa Clara, CA

MARCELO HALPERN
Latham & Watkins
Chicago, IL

J. FRASER MANN
Goldman & Carr L.L.P.
Toronto, Canada

DONALD MACROBERT
Edward Nethan & Friedland, Inc., Sandown, Sandton, South Africa

MICHAEL MCMULDY
Perkins Coie Brown & Bain
Austin, TX

LORELEI S. MASTERS
Anderson, Kill & Olick L.L.P.
Washington, D.C.

EMMANUEL MICHAU
Mchau & Associates
Paris, France

ANTONIO MILLE
Estudio Mille
Buenos Aires, Argentina

LEONARD T. NUARA
Thaxter Profits & Wood
Summit, NJ

RONALD J. PALENSKI
Assistant General Counsel, GTE Technology & Systems
Alhambra, CA

HILARY E. PEARSON
Bird & Bird
London, England

THOMAS J. SMEEDINGHOFF, ESQ.
Wildman Harrold LLP
Chicago, IL

OLIVER R. SMOOT
Executive Vice President, Information Technology Industry Council
Washington, D.C.

LESLEY SUTTON
Reehill Holland & Page
Sydney, Australia

HOLLY K. TOWLE
K & K Gates
Seattle, WA

LUIS VERA
Vera-Abogados S.C.
Mexico D.F., Mexico

BARRY D. WEISS
Cadey Godward
Boulder, CO

STEVE WEINBERG
Steve Weinberg and Weinberg Legal Group
Phoenix, AZ

NICOLE WONG
Associate General Counsel, Google, Inc.
Mountain View, CA

ZACHARY LEVINE
WFL Lawyers
Glendale, CA

e-Commerce Law Report

West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

©2012 Thomson/Reuters

One Year Subscription * 11 Issues * $680.89
(ISSN: PENDING)

For authorization to photocopy, please contact the Copyright Clearance Center at 22 Rosewood Drive, Danvers, MA 01923, USA (978) 750-8400; fax (978) 646-8600 or West’s Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax (651) 687-7551. Please outline the specific material involved, the number of copies you wish to distribute and the purpose or format of the use.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered. However, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

Copyright is not claimed as to any part of the original work prepared by a United States Government officer or employee as part of the person’s official duties.
Work-Life Privacy Balance

The advent of the Internet, smart phones, and tablets has made it possible for users to seamlessly intertwine their work lives and personal lives. Workers can, and are often expected to be accessible 24/7 by e-mail and text messages. Many workers put in a full eight-hour (or more) day, but not necessarily eight contiguous hours.

For many, the ability to be “constantly on” is viewed as a plus—the ability to do work wherever you are. No more having to call into the office or physically go to the office on a set schedule, since you can be contacted anywhere at any time, and you can work on your own pace and on your own schedule. To others it has become the bane of their existence—they are expected to be available whenever their boss or a client wants to find them.

This new working environment has given rise to numerous legal issues that in earlier days would probably not have arisen at all. For hourly employees, how do you calculate how many hours they have “worked”? Is someone working if they are awaiting a call, the receipt of a document, or an important e-mail? And how do you determine how long an employee has worked on a particular day? And can an employee be required to be tethered to his employer constantly, or is she entitled to “free” time where she can be electronically inaccessible?

A second issue is privacy. Today these devices are being used by employees for both work-related and personal communications. Most companies recognize that employees will use their cellphone, laptop, etc. for personal communications during the work day. Often employees are interleaving personal messages with business messages without giving it a second thought. Spouses, children and friends need to be contacted at various times during the day, and workers use the same devices to communicate with them as they do for business communications. What rights do workers have to maintain their private communications in private, even when they are made during the “business day” (whatever that is anymore), using electronic devices supplied by their employers? Do employees have any expectation of privacy in such communications? Should they?

And what about social networking? It is clear to anyone on Facebook, Twitter, or other social networks that people are using them during the business day. Do employees have any privacy rights in what they say on their social networks, or can their employer demand their passwords so their boss can monitor whether they are wasting time that should be devoted to business, are disclosing information on their employer that should be kept confidential, etc.?

Companies, courts, and legislatures are struggling with the appropriate legal rules to govern our increasingly always-on society. While the contours of those laws are not yet clear, what is clear is that people around the world are only going to become more interconnected as time goes by, and that these legal issues need to be hashed out sooner rather than later.

MICHAEL D. SCOTT
EDITOR-IN-CHIEF
WIKI: ITLAW.WIKIA.COM
could not be correct and the court had to focus on whether the defendants accessed information that they were forbidden to access instead of how defendants intended to use the information they had obtained.

Other courts, including the District of Massachusetts, have come to a different conclusion regarding this language in the CFAA. In Guest-Tek Interactive Entertainment Inc. v. Pullen, 665 F. Supp. 2d 42 (D. Mass. 2009), Judge Gorton analyzed a different provision of the CFAA that also included both the “without authorization” and “exceeds authorized access” language. See 18 U.S.C.A. § 1030(a)(4). The defendants argued that the CFAA applies only to those lacking initial authorization and not those who subsequently misuse or misappropriate information. The plaintiff in response argued that the employee defendant’s alleged breach of his fiduciary duty of loyalty to the plaintiff (by copying files and secretly planning a competitive venture while still employed) effectively extinguished his authorization to access plaintiff’s computers. The employee defendant’s initial authorization to access the plaintiff’s confidential information was premised on the agency relationship between the parties, the plaintiff argued, and therefore when the employee breached his duty of loyalty he ended that relationship and constructively terminated his authorization to access the plaintiff’s files. Judge Gorton agreed with the plaintiff. He determined that the First Circuit advocated a broader reading of the CFAA in EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001). In that case, the court upheld a CFAA claim against employees who had collected pricing information from their former employer’s website in order to develop a competing entity with lower prices.” Guest-Tek, 665 F. Supp. 2d at 45. The First Circuit found “that the former employees’ reliance on [plaintiff’s] pricing information reeked of use—and indeed, abuse—of proprietary information that goes beyond any authorized use of [plaintiff’s] website.” Id. (quotation and brackets omitted). The First Circuit’s analysis of the employees’ “authorized use” and “abuse” of the plaintiff’s proprietary information in Explorica, Judge Gorton ruled, undercut the Guest-Tek defendants’ plain language argument—the type of argument the court accepted in O’Brien.

These two cases show that employers can use the CFAA when employees depart to join or form competing companies, but the CFAA’s usefulness may be limited by the case law in the jurisdiction in which the employer sues. Employers therefore should consider where they can sue and the state of the law in those jurisdictions before filing suit. These cases also call attention to a split in case law that eventually may require resolution by the U.S. Supreme Court.

Legal Process Outsourcing: A Cost-saving Scheme Which Might End Up Costing More

By Victor Lau & Vanja Bulut

Victor Lau (vlau@claytonutz.com) is a Senior Associate and Vanja Bulut is a lawyer in the Sydney, Australia office of Clayton Utz (http://www.claytonutz.com).

Introduction

Litigants are increasingly prepared to consider utilising legal process outsourcing as a way of reducing legal costs. A recent UK case of West African Gas Pipeline Company Ltd v Willbros Global Holdings Inc [2012] EWHC 396 (TCC) provides a timely reminder that unless proper checks and balances are put in place, the use of these services could end up costing more.

Lessons from England

In the West African Gas Pipeline case, the England and Wales High Court found that West African Gas Pipeline Company Ltd (the claimant) had
failed to undertake proper discovery and ordered it to pay the defendant’s wasted costs of £135,000.

In this case, the claimant engaged two external litigation support providers, one of which was based in India, to fulfil its discovery obligations. Over 70,000 documents were discovered initially, with over 72,000 more being discovered over a number of months.

During the review of the initial 70,000 discovered documents, Willbros Global Holdings Inc. (the defendant) noticed that an e-mail from a chain had not been discovered. This then led to an extensive enquiry, which brought to light the inadequacy of the review of the documents carried out by the external litigation support providers, which included:

- problems with the deduplication procedures used by the external litigation support providers, leading to a large number of duplicated documents which had not been properly identified and removed;
- failure to deal with redactions consistently; and
- failure to gather together all the documents required to be discovered, and then carry out a proper review process.

The High Court noted that while there must be “some give and take” between parties in relation to difficulties which arise out of discovery, the court may properly exercise its discretion to make costs orders where there had been “a mistake or error which has had significant consequences in terms of time and cost.”

As a result, Justice Ramsey found that the defendant was entitled to have the costs wasted as it resulted in the defendant having to:

- consider, a number of times, duplicated copies of the same document;
- analyse inconsistent redactions; and
- review documents over a prolonged period which inevitably increased costs for the defendant as the discovery process became disrupted.

Managing your Litigation Support Providers

If external litigation support providers are utilised, care must be taken to retain control of the process in order for the party to avoid incurring additional costs due to inadequate discovery.

Parties who engage an external litigation support provider should consider implementing a process that ensures effective management of document review. Steps that could be implemented include:

- undertaking a sufficient and thorough briefing process to ensure that the team fully understands the issues and the tasks;
- providing supervision of the process, where reviewers can raise questions in respect of particular documents;
- introducing a quality assurance process such as conducting a sample of reviewed documents to ensure the review is undertaken correctly and is consistent; and
- providing regular briefings and feedback sessions.

Effective management of the document review would aim to minimise the need to carry out unnecessary additional work.

Defending Your Brand in the .xxx World

Anthony Lupo (lupo.anthony@arentfox.com) is a partner and Amy E. Salomon (salomon.amy@arentfox.com) is an associated in the Washington, D.C. office of Arent Fox.

Since December 6, 2011, when .xxx domains became generally available for registration, brand owners and public figures have faced the reality that their trademarks and personal names may be registered by cybersquatters looking to make a quick buck, or by members of the adult entertain-
ment industry who will use the name/mark with a pornographic website. While there are several new dispute resolution options available to such rights holders, including the Rapid Evaluation Service (RES) and the Charter Eligibility Dispute Resolution Policy (CEDRP), it is becoming clear that the traditional Uniform Domain Name Dispute Resolution Policy (UDRP) is still a viable option to recover domains under this new generic top level domain.

To date, the World Intellectual Property Organization (WIPO) has had ten .xxx domain name cases before it, and the National Arbitration Forum (NAF) has had seven. Of the seven cases before the National Arbitration Forum, two (heb.xxx and richardbranson.xxx) have resulted in the transfer of the domains, while one (foxstudios.xxx) was withdrawn. The remaining four cases are currently pending. Before WIPO, the statistics are similar; one case was terminated without transfer (valero.xxx), one domain was successfully transferred to the complainant (denizbank.xxx), and the remaining eight cases are still pending.

While we are early in the enforcement process for .xxx domains, some patterns are becoming evident. In the case of heb.xxx, where the panel ordered the transfer of the domain to the trademark owner, the respondent failed to make active use of the domain name and was not a member of the adult entertainment industry. Similarly, in the case of richardbranson.xxx, the registrant had no plans to commercialize or make active use of the domain name and was not a member of the adult entertainment industry.

These decisions indicate that brand owners and public figures will have an easier time winning cases where the registrants are not members of the adult entertainment industry and are not making active use of the domains. It is also clear from these decisions that UDRP panels can, and will, consider both RES and CEDRP provisions when deciding a UDRP case, including the rule that a .xxx registrant must be a member of the adult entertainment industry (or a pre-existing rights holder). What remains to be seen, however, is how UDRP cases will be decided when the registrant is a member of the adult entertainment industry and is making active use of the website in connection with adult content.

Given the expense and uncertainty of recovering a domain registered by a cybersquatter or a member of the adult entertainment industry, brand owners should strongly consider applying for .xxx domain names incorporating their trademarks, company names, popular product/service names, and the like, through domain name registrars. For assistance with this process or with enforcement options once a third party registers your name or brand in a .xxx domain, please contact the attorneys listed at right.

Will the Pinterest “Nopin” Tag Put Online Image Owners on the Defensive on Implied Copyright Licenses? Should We Look to Robots.txt as Precedent?

BY JEFF NEUBURGER

Jeff Neuberger (jneuburger@proskauer.com) is a partner in the New York office and Cochair of the Technology, Media and Communications Practice Group at Proskauer Rose. Copyright © 2012, Proskauer Rose LLP. All Rights Reserved.

Pinterest is the hot, hot, hot, social media site that lets users create online “pinboards” of interesting or inspiring images. Although users may upload their own images to their pinboards, Pinterest emphasizes the pinning of images from third-party Web sites through the use of inline links.
This of course generates yet a new series of online copyright issues. Although Pinterest can drive traffic to the third-party sites, and some content owners are happy about that, the love of Pinterest is not universal. Many believe that traffic coming from Pinterest as a result of their images being pinned on the site is minimal. One commentator has referred to Pinterest as “the new Napster” and suggested that 99% of the “pins” on the site are in violation of the site’s Terms of Service (requiring the user to have right to “pin” an image.)

Pinterest announced in February that it had implemented a technological measure to address copyright concerns, the “nopin” tag. The code, when implemented on a content-owner’s Web site, blocks attempts to pin that site’s images via inline linking. When a Pinterest user attempts to pin an image from the target site, the code generates a message informing the Pinterest user that the target site doesn’t allowing pinning. (Note that the “nopin” code does not inhibit the ability of a Pinterest user to download an image from a target site and then upload the image to Pinterest as the user’s own image.)

The availability of the “nopin” tag raises many legal issues. Does a site have an obligation to use the “nopin” tag to prevent pinning of its images? Does the failure to use the tag constitute the grant of an implied license to pin? What role do the restrictions on use found in the target site’s terms and conditions play in all of this? Could the failure to deploy a “nopin” tag impair a copyright holder’s ability to utilize the DMCA takedown procedure to remove infringing images from Pinterest?

Although many copyright holders would quickly say “no, of course I do not have an obligation to use the nopin tag,” it is interesting to look at a similar issue that has been litigated in the context of the “robots.txt” protocol. The robots.txt protocol allows site owners to indicate whether, and to what extent, they consent to having their sites crawled and cached by Web crawlers and spiders that are utilized not only by major search engines like Google and Yahoo! but also by price comparison sites or even the competitors of the crawled sites.

In Field v. Google, Inc., 412 F. Supp 2d. 1106 (D. Nev. 2006), a claim of copyright infringement stemming from search engine crawling and caching was rejected based upon the lack of a robots.txt file on the copyright owner’s site. The court concluded that the content owner’s knowing failure to deploy a robots.txt file that said “no” to crawling and caching had given search engines an implied license to crawl and cache. It should be noted that the court believed the plaintiff had deliberately invited the crawling and caching and was acting in less than good faith. However, a similar result was reached on more balanced facts in Parker v. Yahoo!, Inc., 2008 U.S. Dist. LEXIS 74512 (E.D. Pa. Sept. 26, 2008). In neither of these cases did the courts consider the crawled sites’ terms of use, if any.

Is the failure to use robots.txt a grant of an implied license to spider and cache? Could the failure to deploy the nopin tag similarly be considered the grant of an implied license? If so, when the non-deploying copyright holder sends a DMCA takedown notice, could Pinterest or the user argue that they were acting pursuant to an implied license (and thus the notice was improper)? To the extent that the terms of use prohibit commercial use or linking, would that be viewed as superseded by the site’s failure to deploy the “nopin” tag?

There is a very significant difference between Pinterest’s “nopin” code and the robots.txt protocol, at least at the present time. The robots.txt protocol is a long-established and widely accepted standard acknowledged by Web professionals. The courts in Field v. Google and Parker v. Yahoo! both relied on the widespread acceptance of the robots.txt protocol in their rulings. The Pinterest “nopin” code, however, is being promulgated unilaterally by a single Web site operator with an obvious interest in putting the burden on content owners to take action to protect their content. But given the widespread popularity of Pinterest, and the inevitable launch of numerous copycat sites with similar nopin-type codes, this type of code has the potential to develop into a de facto standard for controlling content sharing.

The interplay between codes like “nopin,” the robots.txt precedent, the doctrine of implied li-
censing, the DMCA and the role of Web site terms of use, is likely to receive increased legal attention and could be the basis of some interesting litigation in the near future.

Germany: E-commerce Obligations—Order Buttons Need to be Changed

By Dr. Fabian Niemann & Stefan Kujat

Dr. Fabian Niemann (fabian.niemann@twobirds.com) is a partner and Stefan Kujat (stefan.kujat@twobirds.com) is an associate in the Frankfurt am Main, Germany office of Bird & Bird LLP.

On 2 March 2012, the German Federal Parliament (Deutscher Bundestag) adopted a new law that imposes far-reaching additional obligations on e-commerce providers in business-to-consumer transactions.

Under the new legislation, e-commerce contracts between e-commerce providers and consumers are only valid if the order process is designed in a way that requires the consumer, when placing the order, to expressly confirm that they are under an obligation to pay. An order button used to complete the transaction must be labelled with the wording “zahlungspflichtig bestellen” (order with an obligation to pay) or something equally unambiguous. Merely labelling a button with “I accept” will no longer be sufficient.

In addition, this new law tightens the e-commerce provider’s information obligations relating to important characteristics of the product or the service, the minimum term of the contract (if any), as well as the price, taxes and costs of the product or the service.

Both obligations do not apply to business-to-business transactions. While noncompliance with the information obligations does not automatically make the contract invalid (but can, inter alia, lead to injunction claims by competitors or consumer protection agencies), an incorrect design of the order button will render a contract, null and void.

Failing to implement a compliant order button after the new law has become effective will lead to a loss of all contractual payment claims against consumers, e-commerce providers are thus encouraged to react quickly.

The new German legislation will enter into force as early as the first day of the third month following its official promulgation and will therefore become effective in the second or third quarter of 2012. In principle, it can be seen as a very early step of a transposition of Art. 8 para 2 of the new EU Directive 2011/83/EU on consumer rights which is due to be implemented into the EU Member States’ national laws by December 2013.

NTIA Requests Comments on the Development of Consumer Data Privacy Codes of Conduct

By Stephanie M. Phillipps, William E. Cook, Jr. & Michael Levin

Stephanie M. Phillipps (Stephanie.Philippps@aporter.com) and William E. Cook, Jr. (William.Cook@aporter.com) is a partner in the Washington, D.C. office of Arnold & Porter LLP. Michael Levin (Michael.Levin@aporter.com) is an associate in the firm’s New York City office. © 2012 Arnold & Porter LLP. Published with permission.

The National Telecommunications and Information Administration (NTIA) is requesting comments on consumer data privacy issues that
should be included as part of legally enforceable consumer data privacy codes of conduct, as well as procedures for the development of such codes. Comments are due on or before March 26, 2012.

On February 23, 2012, the White House released Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, which included a Consumer Privacy Bill of Rights setting forth the principles that should govern the handling of personal data in commercial sectors. Pursuant to that Framework, NTIA is tasked with convening a multistakeholder process for the development of legally enforceable codes of conduct addressing how the Consumer Privacy Bill of Rights will apply in specific business contexts.

The Request is NTIA’s first step in that process. NTIA seeks public comment from “all stakeholders with an interest in consumer data privacy, including the commercial, academic, and civil society sectors, and from federal and state enforcement agencies.” NTIA’s role in the privacy multistakeholder process will be “to provide a forum for discussion and consensus-building among stakeholders,” and to help the stakeholders “reach clarity on what their positions are and whether there are options for compromise toward consensus, rather than substituting its own judgment.”

A company’s decision to adopt a code of conduct will be voluntary. However, if a company affirmatively commits to follow a code, NTIA stated that it expects the commitment will be legally enforceable, provided the company is subject to the jurisdiction of the Federal Trade Commission (FTC). NTIA stated that the FTC will likely have the authority to enforce the code under 15 U.S.C. § 45, which gives the FTC authority to prevent deceptive acts or practices.

NTIA requests comments on the topics below.

### Which Consumer Data Privacy Issues Should Be Addressed By the Codes of Conduct?

NTIA intends to conduct an initial privacy multistakeholder process focused on a “definable area where consumers and businesses will receive the greatest benefit in a reasonable timeframe.” The Request cites “transparency” as a possible starting point because, according to NTIA, there was “broad agreement” among commenters on the Department of Commerce’s December 2010 “Privacy and Innovation Green Paper” that transparency is “a key element of protecting consumers’ privacy.”

Thus, NTIA seeks comment on whether it should convene an initial stakeholder process to “facilitate the implementation of the Transparency principle in the privacy notices of mobile device applications (‘mobile apps’).” The “Transparency principle” is one of the seven privacy rights set forth in the White House’s Consumer Privacy Bill of Rights. It provides, in relevant part, that “[c]onsumers have a right to easily understandable and accessible information about privacy and security practices.” NTIA stated that a “common set of practices” that implement the Transparency principle “could provide guidance to mobile apps developers, operating systems, and apps stores, as well as better inform consumers about how mobile apps use personal data.”

NTIA also seeks comments on other potential topics, including, but not limited to:
- other issues associated with mobile apps in general;
- mobile apps that provide location-based services;
- cloud computing services;
- mechanisms for accountability in the implementation of the Consumer Privacy Bill of Rights;
- online services directed towards teenagers and/or children;
- trusted identity systems; and
- the use of multiple technologies to collect personal data.

### How to Implement the Multistakeholder Process?

NTIA seeks comment on how the multistakeholder process should be structured to ensure
openness, transparency, and consensus-building. Possible areas for comment include, among others:

- How can NTIA promote participation by a broad range of stakeholders?
- Should there be pre-requisites for participating in the process consistent with the principle of openness?
- How can NTIA ensure transparency in the process?
- How can NTIA facilitate broad public review of codes of conduct during their development?
- What procedures should stakeholders follow to explain their decisions?
- How to define consensus?
- How can NTIA encourage stakeholders to reach consensus?

NOTES


3. Request, at 13098.
4. Id.
5. Id.
6. Id. The FTC’s jurisdiction covers the “organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce, excepting banks, savings and loan institutions described in section 57a(f) (3) of this title, Federal credit unions described in section 57a(f)(4) of this title, and common carriers.” Federal Trade Commission Act, 15 U.S.C.A. § 46(a).
7. Request, at n.3.
8. Id. at 13099.
10. Request, at 13099.
12. Id.
13. Request, at 13099.

FTC

FTC Gets Court Order Shutting Down Pyramid Scam

At the request of the Federal Trade Commission, a U.S. district court judge has ordered the operators and top promoters of a deceptive pyramid scheme to pay a total of $17 million to refund consumers who were burned by the scam. The court order permanently halts marketing methods used by the operation known as BurnLounge, which lured more than 56,000 consumers from around the country by masquerading as a legitimate multi-level marketing program and making misleading claims about earnings to be made.

The FTC filed a complaint against BurnLounge in 2007 as part of its ongoing efforts to protect consumers from fraud and deception. BurnLounge had touted itself as a cutting-edge way to sell digital music through multi-level marketing, but music sales accounted for only a small percentage of its sales. The agency charged that BurnLounge recruited consumers from across the country by telling them that participants earned huge incomes. Investors could buy into the BurnLounge organization for prices ranging from $29.95 to $429.95, plus monthly fees. While participants were compensated for music and album sales, most compensation came from recruiting others into the plan.

The FTC charged the defendants with operating an illegal pyramid scheme, with making deceptive earnings claims, and with failing to dis-
close that most consumers who participated in pyramid schemes would not receive substantial income, but instead would lose money. The agency charged that the practices violate federal law.

The court’s final judgment and order bars the defendants from engaging in pyramid, Ponzi, or chain letter schemes or any schemes in which compensation for recruitment is unrelated to the sale of product to customers who are not participants. The order bars misrepresentations about multilevel marketing operations or business ventures, including misrepresentations about sales, income, profitability, or legality of the operations. If the defendants make claims about earnings, sales, or profits, the order requires them to disclose the number and percentage of participants in the business venture who have earned, sold or profited that much.

Finally, the court ordered the defendants to pay, collectively, close to $17 million for consumer redress. BurnLounge, Inc., and Juan Alexander Arnold were ordered to pay $16,245,799. John Taylor was ordered to pay $620,138 and Rob DeBoer was ordered to pay $150,000. Standard bookkeeping and record keeping requirements in the order will allow the FTC to monitor compliance.

In June 2007, another defendant in the pyramid scheme, Scott Elliott, settled the FTC’s charges against him. The settlement barred him from participating in any pyramid scheme or other prohibited marketing scheme, barred false earning claims, and required him to give up $20,000 in ill-gotten gains.

---

**FTC Approves Safe Harbor Program Under COPPA for Aristotle International, Inc.**

The Commission has approved Aristotle International, Inc. as a “safe harbor” program under the terms of the Children’s Online Privacy Protection Act of 1998 (COPPA). COPPA’s “safe harbor” provision is designed to provide flexibility and promote efficiency in complying with the Act by encouraging industry members or groups to develop their own COPPA oversight programs. Operators that participate in a COPPA safe harbor program will, in most circumstances, be subject to the review and disciplinary procedures provided in the safe harbor’s guidelines in lieu of formal FTC investigation and law enforcement.

The FTC’s COPPA Rule requires that operators of commercial websites and online services directed to children under the age of 13, or general-audience Web sites and online services that knowingly collect personal information from children under 13, must post comprehensive privacy policies on their sites, notify parents about their information practices, and obtain parental consent before collecting, using, or disclosing any personal information from children under the age of 13. COPPA also directed the Commission to review and approve self-regulatory program guidelines that would serve as safe harbors.

To be approved by the FTC, proposed safe harbor guidelines must fulfill three criteria: (1) provide the same or greater protections for children as those contained in the Rule; (2) set forth effective, mandatory mechanisms for the independent assessment of members’ compliance; and (3) provide effective incentives for members’ compliance.
FTC Stops Deceptive Practices of Marketer Who Used Bogus ‘Free’ Trial Offers

The Commission has stopped an Internet scheme that allegedly used bogus “free” product offers that deceived consumers in the United States and other countries and charged them for products and services they did not want or agree to purchase. Almost four million consumers fell prey to the lure of these “free trial” offers.

According to the FTC’s complaint, Willms and his companies lured consumers with “free” trial offers for weight-loss pills, teeth whiteners, health supplements, a work-at-home scheme, access to government grants, free credit reports, and penny auctions. Consumers were often charged for the “free” trial, a monthly recurring fee, typically $79.95, and additional monthly recurring fees for so-called “bonus” offers. The defendants allegedly contracted with affiliate marketers whose banner ads, pop-ups, sponsored search terms, and unsolicited e-mail led consumers to the defendants’ Web sites, and paid the affiliates for each consumer whose credit or debit card was charged. The agency filed an amended complaint, in September 2011, to add two defendants.

The settlement order permanently bans Jesse Willms and his companies from using “negative-option” marketing, a practice in which the seller interprets consumers’ silence or inaction as permission to charge them. The Willms settlement order imposes a judgment of $359 million that will be suspended upon Willms’ surrender of bank account funds and proceeds from the sale of his house, personal property, and corporate assets, including a Cadillac Escalade, fur coat, and artwork.

The Willms settlement order also permanently prohibits Willms and his 11 companies from:

- debiting consumers’ bank accounts without first obtaining their express verifiable authorization;
- misrepresenting any product or service or the terms and conditions associated with any offer, specifically including claims of “free,” “risk-free,” or “trial offer”;
- failing to clearly disclose the terms and conditions of any offer, including refund terms, before requesting consumers’ payment information;
- making misleading or unsubstantiated disease-prevention, weight-loss, and other health-related claims;
- using false or deceptive endorsements and testimonials;
- failing to monitor the activities of marketing affiliates and affiliate networks involved in the marketing of any Willms product or service; and
- making misrepresentations in order to obtain services from payment processors, banks, and other third parties.

In addition to Willms and his companies, five individuals who allegedly provided services to Willms have entered into separate settlements with the FTC. They are permanently prohibited from making misrepresentations in order to obtain services from payment processors, banks, and other third parties. The amended complaint alleged that these defendants, along with Willms, provided merchant banks with false or misleading information to obtain and maintain merchant accounts through which Willms placed charges on consumers’ credit and debit card accounts.

The settlement orders against these individuals also impose monetary judgments of varying amounts.
EA Denied SSX.com

By Davis LLP Videogame Law Group

For further information, contact Chris Bennett at cbennett@davis.ca or go to www.videogamelawblog.com. The other members of the Davis LLP Videogame Law Group are Tudor Carsten, Sarah Dale-Harris, Pablo Guzman, Michael R. Coburn, Meika Lalonde, Michael L. Mjanes and Craig K. Natsuhara.

EA Lawsuit - Further Thoughts

By David Spratley

We published last month about how EA has brought a pre-emptive lawsuit seeking judicial confirmation that it has a constitutional right to depict real-world helicopters in its games. This lawsuit is another example of the issues involved in depicting real-world brands and objects in video games. We discussed this topic in more detail some time ago.

The EA dispute is interesting because apparently the helicopter manufacturer demanded that EA cease depicting its helicopters in the Battlefield 3 game, and the parties could not reach a resolution. EA then filed its pre-emptive lawsuit on freedom of speech and nominative fair use grounds. (Nominative fair use is a U.S. trademark principle that says it is OK to refer to a third-party trademark in order to identify that party’s products, services, or business, so long as you do not suggest an endorsement or affiliation.)

Presumably the helicopter manufacturer takes the position that its choppers are distinctive, that it has trademark rights in them, and that any unauthorized depiction of them infringes these rights. The strength of this position is not clear, and EA’s lawsuit, if it proceeds, will shed more light on the legality of depicting real-world objects in video games.

Further to its analysis of the parties’ submissions, the National Arbitration Forum found, inter alia, that the Respondent has rights or legitimate interests in the SSX.com domain name and that it did not register or use the disputed domain name in bad faith. The Forum therefore found that EA failed to establish each of the three elements required under the ICANN Policy to have the domain name transferred or cancelled and denied the relief sought.

Fallout From Bethesda-Interplay Lawsuit Dissipates

(SUBMITTED BY DAVID SPATLEY)

Bethesda and Interplay have settled a long-running dispute over the Fallout IP. Bethesda bought the Fallout franchise from Interplay in 2007, but licensed back to Interplay certain rights to sell pre-existing Fallout games and to develop and operate a Fallout-based MMO. The MMO portion of the licence contained various conditions, including that Interplay secure funding and start full-scale development of the MMO within two years, and launch the MMO within four years.

In 2009, Bethesda launched a lawsuit against Interplay for trade-mark infringement (on the basis that Interplay was not complying with the trade-mark provisions of the 2007 licence in its activities relating to the pre-existing Fallout games) and breach of contract (on the basis that Interplay had not begun developing the MMO).

Reports are that the settlement includes the cancellation of the MMO licence and the reversion of all MMO-related rights to Bethesda, the cancellation of any other Fallout-related IP rights granted to Interplay, and a $2 million payment by Bethesda to Interplay.
### Calendar of EVENTS

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 3-4, 2012</td>
<td>San Francisco, CA</td>
<td>Information Technology Law Institute 2012: Navigating the New Risks in Mobile Technology, Social Media, Electronic Records and Privacy</td>
</tr>
<tr>
<td>April 19, 2012</td>
<td>Palo Alto, CA</td>
<td>Venture Capital 2012: Nuts and Bolts</td>
</tr>
<tr>
<td>April 26-27, 2012</td>
<td>Chicago, IL</td>
<td>Advanced Licensing Agreements 2012</td>
</tr>
<tr>
<td>May 10-11, 2012</td>
<td>Houston, TX</td>
<td>Current Issues in IP Licensing</td>
</tr>
<tr>
<td>August 27-28, 2012</td>
<td>Seattle, WA</td>
<td>Current Issues in IP Licensing</td>
</tr>
<tr>
<td>June 11, 2012</td>
<td>San Francisco, CA</td>
<td>Cloud Computing 2012: Cut Through the Fluff &amp; Tackle the Critical Stuff</td>
</tr>
<tr>
<td>May 17-18, 2012</td>
<td>Atlanta, GA</td>
<td>Mobile Payment Systems</td>
</tr>
<tr>
<td>August 16-17, 2012</td>
<td>Seattle, WA</td>
<td>Mobile Payment Systems</td>
</tr>
</tbody>
</table>

**For information:** Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

**For information:** Law Seminars International, 800 Fifth Avenue, Suite 101, Seattle, WA 98104; Tel.: (206) 567-4490 or (800) 854-8009; E-mail: registrar@lawseminars.com.
Calendar of EVENTS

May 21-22, 2012  San Francisco, CA
June 18-19, 2012  New York, NY
July 16-17, 2012  Chicago, IL

Privacy and Data Security Law Institute (Thirteenth Annual)
For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

May 24-25, 2012  Seattle, WA

Internet-Based Health Care
For information: Law Seminars International, 800 Fifth Avenue, Suite 101, Seattle, WA 98104; Tel.: (206) 567-4490 or (800) 854-8009; E-mail: registrar@lawseminars.com.

June 11, 2012  Seattle, WA

Data Rights
For information: Law Seminars International, 800 Fifth Avenue, Suite 101, Seattle, WA 98104; Tel.: (206) 567-4490 or (800) 854-8009; E-mail: registrar@lawseminars.com.

June 14, 2012  Chicago, IL
July 9, 2012  San Francisco, CA
July 16, 2012  New York, NY

Understanding Copyright Law in the Data Era 2012
For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

June 15, 2012  Chicago, IL
July 10, 2012  San Francisco, CA
July 17, 2012  New York, NY

Understanding Trademark Law in the Global Marketplace 2012
For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

June 15, 2012  Chicago, IL
July 10, 2012  San Francisco, CA
July 17, 2012  New York, NY

September 6-7, 2012  Seattle, WA

Social Media Law
For information: Law Seminars International, 800 Fifth Avenue, Suite 101, Seattle, WA 98104; Tel.: (206) 567-4490 or (800) 854-8009; E-mail: registrar@lawseminars.com.

September 7, 2012  New York, NY
September 19, 2012  San Francisco, CA

Technology and Entertainment Convergence 2012: Hot Business and Legal Issues in “Technotainment”
For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

September 24, 2012  New York, NY

Electronic Discovery Guidance 2012: What Corporate and Outside Counsel Need to Know
For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.
Calendar of EVENTS

October 1-2, 2012   Chicago, IL
October 29-30, 2012   New York, NY

Outsourcing 2012: Structuring, Negotiation and Governance

For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

October 4-5, 2012   Seattle, WA

Gamer Technology Law

For information: Law Seminars International, 800 Fifth Avenue, Suite 101, Seattle, WA 98104; Tel.: (206) 567-4490 or (800) 854-8009; E-mail: registrar@lawseminars.com.

October 11-12, 2012   Philadelphia, PA

Privacy By Design

For information: Law Seminars International, 800 Fifth Avenue, Suite 101, Seattle, WA 98104; Tel.: (206) 567-4490 or (800) 854-8009; E-mail: registrar@lawseminars.com.

October 17, 2012   San Francisco, CA

Representing the Games Industry Client 2012

For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

October 18-19, 2012   New York, NY
November 8-9, 2012   Chicago, IL
December 10-11, 2012   San Francisco, CA

Understanding the Intellectual Property License 2012

For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

November 5, 2012   New York, NY

Think Like a Lawyer and Ask Questions Like a Geek: Understanding Cybersecurity, Social Media and Mobile Technology 2012

For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

November 13, 2012   San Francisco, CA

Tracking and Targeting Customers and Prospects Online and in Social Media 2012

For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

November 14, 2012   New York, NY
December 5, 2012   San Francisco, CA

Open Source and Free Software 2012: Benefits, Risks and Challenges

For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.
November 15-16, 2012   New York, NY

Communications Law in the Digital Age 2012

For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.

December 4, 2012   San Francisco, CA

Advanced Venture Capital 2012

For information: Practising Law Institute, 810 Seventh Avenue, New York, NY 10019-5818. Tel.: (800) 260-4PLI or (212) 824-5710; E-mail: info@pli.edu.
Master the practice and business of law as you grow in your profession with legal curriculum and training from West LegalEdcenter. Get unparalleled breadth and depth of content from one source, organized with you and your associates at the center.

westlegaledcenter.com
1.800.241.0214
YES! Rush me e-Commerce Law Report and enter my one-year trial subscription (11 issues) at the price of $680.89. After 30 days, I will honor your invoice or cancel without obligation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Street Address</th>
<th>City/State/Zip</th>
<th>Phone</th>
<th>Fax</th>
<th>E-mail</th>
</tr>
</thead>
</table>

**METHOD OF PAYMENT**

- [ ] Check enclosed (to West Legalworks)
- [ ] BILL ME
- [ ] VISA
- [ ] MASTERCARD
- [ ] AMEX

<table>
<thead>
<tr>
<th>Account #</th>
<th>Exp. Date</th>
<th>Signature</th>
</tr>
</thead>
</table>

Postage charged separately. All prices are subject to sales tax where applicable.