ALSTON+BIRD LLP
WWW.ALSTON.COM

Agenda

8:30 - 9:00 a.m.	**Networking Continental Breakfast**
9:00 - 9:45 a.m.	**What Should I Be Doing About Data Security and Privacy Right Now?** Tom Arbogast, Vice President and Director of Commercial Collaboration, BT Design Jon Gordon, Partner, Alston & Bird LLP Todd McClelland, Partner, Alston & Bird LLP Michael Zweiback, Partner, Alston & Bird LLP
9:45 - 10:15 a.m.	**Who Changed My Backend? – Issues raised by the continued adoption of cloud computing and open source** David Teske, Partner, Alston & Bird LLP Todd McClelland
10:15 - 10:40 a.m.	**Break**
10:40 - 11:10 a.m.	**Where Did That Content Come From? – Implications of targeted marketing and user generated content** Katherine Wallace, Partner, Alston & Bird LLP
11:10 - 11:25 a.m.	**Legislative Update – Privacy and Data security** Paul Martino, Partner, Alston & Bird LLP
11:25 - 12:00 p.m.	**Botnets, Pirates and Cybercriminals – What are the current trends?** James Aquiliana, Executive Managing Director and Deputy General Counsel, Stroz Friedberg LLC Mark Ishikawa, Chief Executive Officer, BayTSP, Inc. David Teske

What Else Should be Keeping You Up at Night – Current Uses and Abuses of the Internet

March 31, 2009
Los Angeles, CA

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

- **A Panel Discussion: Issues and Scenarios**

Jon Gordon, Alston + Bird, LLP, Moderator

Tom Arbogast, BT, VP and Director Commercial Collaboration for BT Design

Todd McClelland, Alston + Bird, LLP

Mike Zweiback, Alston + Bird, LLP

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

Tom Arbogast, BT Design

Tom is Vice President and Director of Commercial Collaboration for BT Design, BT's IT arm, comprised of nearly 20,000 global employees. He handles major IT supplier, customer and outsourcing negotiations and oversees the implementation of large IT projects from a commercial perspective. Prior to joining BT, he served as an Executive Vice President for a small telco and also worked in a business development/commercial-legal capacity for a large professional services consulting company. He previously worked as appellate counsel in Canada and has argued numerous cases before the Supreme Court of Canada and the BC Court of Appeal.

Todd McClelland, Alston & Bird, LLP

Todd McClelland specializes in strategic corporate projects that include significant technology, IP, outsourcing, or energy components. His practice scope includes IT systems procurement and infrastructure, outsourcing projects, energy policy, construction projects, intellectual property management, business model innovation activities and technology and energy company representation. In addition to his transactional practice, Todd is a registered patent attorney and provides counsel on patent licensing, avoidance and procurement.

Michael Zweiback, Alston & Bird, LLP

Michael Zweiback is a partner in the firm's Los Angeles office focusing his practice on governmental and corporate investigations, white collar criminal defense, environmental crimes, privacy and data security matters. He joins the firm from the U.S. Attorney's Office in Los Angeles, where he had been chief of the Cyber and Intellectual Property Crimes Section since 2007.

Jonathan Gordon, Alston & Bird, LLP

Jonathan Gordon, partner in the firm's Los Angeles office, advises clients involved in the commercialization of new technologies, intellectual property and licensing transactions, and technology research and development. He counsels clients on their business transactions and practices over the Internet. Mr. Gordon also handles disputes involving licenses, patents, copyrights, trademarks and trade secrets, as well as other business disputes. He has represented clients in state and federal courts and in a variety of domestic and international arbitration forums.

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #1: Laptops– Should we lock them back into their docking stations?**

  Company employees globe-trotting and vacationing with their laptops containing PII (personally identifiable information) and Company trade secrets: What do you do when the laptop is stolen, hacked or searched at a border? What measures should you be taking now?

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario # 2: Printed medical and personal data in the dumpster– the FTC case against CVS.**

  CVS Caremark stores were alleged to have regularly put in dumpters pill containers and documents containing personal medical information, social security numbers, payroll information, insurance cards, account numbers, driver's license numbers and HIPAA-protected information. Multi-faceted remedies enforced by FTC, including 20 years of audits and $2.25MM payment.

What Should I Be Doing About Data Security and Privacy Right Now?

DATAFLOW Analysis and Software Development Lifecycle

- The traditional "CIA" model for analyzing information in a data/IT context addresses: Confidentiality / Integrity / Availability
- From a project, or ground-up perspective, this can be viewed as:
- Concurrency / Iteration / Accessibility
- It is important to understand the stages of the Software Development Lifecycle. This will in turn lead to an understanding of DATAFLOW

What Should I Be Doing About Data Security and Privacy Right Now?

DATAFLOW Chart Considerations:

- Creation and Collection
- Storage and Handling (Classification)
- Migration and Transit (and accessibility in context)
- Conversion and Use
- Restrictions (Legal, Regulatory, Policy and Business)
- Retention and Destruction Requirements
- Authorization and Administration Policy

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

Agile Development and Iterative Cycles for DATAFLOW Analysis

- Requirements Analysis
- Design and Build
- Implement
- Test
- These steps are becoming iterative and repeatable and require concurrent input from Legal/Regulatory to properly monitor privacy and security issues

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #3: What responsibility do you have for third parties who have access to your systems or data?**

  A mortgage lender in Texas allowed its database to be accessed by a third party home-seller. Third party was then hacked and lender's database was compromised allowing access to credit reports and personal financial information of lender's customers. FTC imposes comprehensive remedies including 20 year requirements.

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #4: No breach ≠ no enforcement**

  London stockbroker had "casual" practices regarding customer personal and financial information over phone calls, published in unsecured mailings, and stored as unencrypted data at employees' homes. There was no known breach or theft of this data. FSA (UK Financial Services Authority) enforces fine and remedies.

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #5: Heartburn at Heartland**

100 million credit card records compromised when a weak point in the company's data flow process is attacked and un-encrypted data is accessed. What are the costs of security incidents?

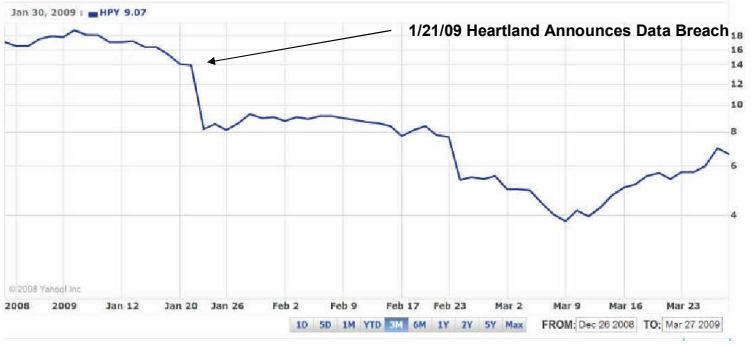
What Should I Be Doing About Data Security and Privacy Right Now?

YAHOO! FINANCE **Heartland Payment Systems Inc. (HPY)**

7.02	Open:	6.27	Mkt Cap:	262.84M	P/E:	6.49	Dividend:	0.03
+1.01 (16.81%)	High:	7.18	52Wk High:	33.00	F P/E:	-	Yield:	1.42
Mar 26 - Close	Low:	6.19	52Wk Low:	3.57	Beta:	1.47	Shares:	37.44M
	Vol:	908,223.00	Avg Vol:	738,000.00	EPS:	1.08	Inst. Own:	74%

After Hours: 7.02 0.00 (0.00%) - Mar 26, 5:01PM EDT

NYSE Real-time data - Disclaimer



What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #6: A "logic bomb" at Fannie Mae and the hazards of the "hack back."**

  A trusted employee/contractor is being terminated and, on the way out the door, he plants a logic bomb into the company's server that will literally destroy all data on 4,000 company servers. Miraculously discovered "by accident, " detonation of the bomb was averted.

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #7: Cloud computing– the wave of the future has a tsunami of data security issues**

  Everyone is singing the praises of "the cloud" to cut costs and enable applications. But, is the cloud secure? How do you monitor and control your risks? Who are you dealing with, where is the infrastructure and who is accountable?

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario # 8: New state enforcement schemes everywhere you turn– how do you manage this?**

  New state legislation is coming fast and furious from many jurisdictions (e.g., California, Massachusetts, New York, Nevada, Connecticut, Texas, New Jersey), layered on top of the FTC, and HIPAA regimes, not to mention the EU Data Directive and global regulation. How do you respond and manage this and what does the future hold?

Supporting Materials

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellant,* v. MICHAEL TIMOTHY ARNOLD, *Defendant-Appellee.*	No. 06-50581 D.C. No. CR-05-00772-DDP ORDER AND AMENDED OPINION

Appeal from the United States District Court
for the Central District of California
Dean D. Pregerson, District Judge, Presiding

Argued and Submitted
October 18, 2007—Pasadena, California

Filed April 21, 2008
Amended July 10, 2008

Before: Diarmuid F. O'Scannlain and Milan D. Smith, Jr.,
Circuit Judges, and Michael W. Mosman,* District Judge.

Opinion by Judge O'Scannlain

*The Honorable Michael W. Mosman, United States District Judge for the District of Oregon, sitting by designation.

COUNSEL

Steve Kim, Assistant United States Attorney, Criminal Appeals Section, Los Angeles, California, argued the cause for the plaintiff-appellant and filed briefs; George S. Cardona, United States Attorney, and Thomas P. O'Brien, Assistant United States Attorney, Chief, Criminal Division, Los Angeles, California, were on the briefs.

Marilyn E. Bednarski, Kaye, McLane, & Bednarski, LLP, Pasadena, California, argued the cause for the defendant-appellee and filed a brief; Kevin Lahue, Kaye, McLane, & Bednarski, LLP, Pasadena, California, was on the brief.

ORDER

The opinion filed April 21, 2008, is amended as follows:

1. At 523 F.3d 941, 946 n.1 (9th Cir. 2008), in the first sentence replace "incoming" with "outgoing."

With the foregoing amendment, the panel has unanimously voted to deny the petition for rehearing. Judge O'Scannlain and Judge M. Smith, Jr., vote to deny the petition for rehearing en banc and Judge Mosman so recommends. The full court has been advised of the petition for rehearing en banc and no active judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petition for rehearing and the petition for rehearing en banc are DENIED. Further petitions for rehearing or rehearing en banc may not be filed.

OPINION

O'SCANNLAIN, Circuit Judge:

We must decide whether customs officers at Los Angeles International Airport may examine the electronic contents of a passenger's laptop computer without reasonable suspicion.

I

On July 17, 2005, forty-three-year-old Michael Arnold arrived at Los Angeles International Airport ("LAX") after a nearly twenty-hour flight from the Philippines. After retrieving his luggage from the baggage claim, Arnold proceeded to customs. U.S. Customs and Border Patrol ("CBP") Officer Laura Peng first saw Arnold while he was in line waiting to go through the checkpoint and selected him for secondary questioning. She asked Arnold where he had traveled, the purpose of his travel, and the length of his trip. Arnold stated that he had been on vacation for three weeks visiting friends in the Philippines.

Peng then inspected Arnold's luggage, which contained his laptop computer, a separate hard drive, a computer memory stick (also called a flash drive or USB drive), and six compact discs. Peng instructed Arnold to turn on the computer so she could see if it was functioning. While the computer was booting up, Peng turned it over to her colleague, CBP Officer John Roberts, and continued to inspect Arnold's luggage.

When the computer had booted up, its desktop displayed numerous icons and folders. Two folders were entitled "Kodak Pictures" and one was entitled "Kodak Memories." Peng and Roberts clicked on the Kodak folders, opened the files, and viewed the photos on Arnold's computer including one that depicted two nude women. Roberts called in supervisors, who in turn called in special agents with the United States Department of Homeland Security, Immigration and

Customs Enforcement ("ICE"). The ICE agents questioned Arnold about the contents of his computer and detained him for several hours. They examined the computer equipment and found numerous images depicting what they believed to be child pornography. The officers seized the computer and storage devices but released Arnold. Two weeks later, federal agents obtained a warrant.

A grand jury charged Arnold with: (1) "knowingly transport[ing] child pornography, as defined in [18 U.S.C. § 2256(8)(A)], in interstate and foreign commerce, by any means, including by computer, knowing that the images were child pornography"; (2) "knowingly possess[ing] a computer hard drive and compact discs which both contained more than one image of child pornography, as defined in [18 U.S.C. § 2256(8)(A)], that had been shipped and transported in interstate and foreign commerce by any means, including by computer, knowing that the images were child pornography"; and (3) "knowingly and intentionally travel[ing] in foreign commerce and attempt[ing] to engage in illicit sexual conduct, as defined in [18 U.S.C. § 2423(f)], in a foreign place, namely, the Philippines, with a person under 18 years of age, in violation of [18 U.S.C. § 2423(c)]."

Arnold filed a motion to suppress arguing that the government conducted the search without reasonable suspicion. The government countered that: (1) reasonable suspicion was not required under the Fourth Amendment because of the border-search doctrine; and (2) if reasonable suspicion were necessary, that it was present in this case.

The district court granted Arnold's motion to suppress finding that: (1) reasonable suspicion was indeed necessary to search the laptop; and (2) the government had failed to meet the burden of showing that the CBP officers had reasonable suspicion to search.

The government timely appealed the district court's order granting the motion to suppress.

II

Arnold argues that the district court was correct in concluding that reasonable suspicion was required to search his laptop at the border because it is distinguishable from other containers of documents based on its ability to store greater amounts of information and its unique role in modern life.

Arnold argues that "laptop computers are fundamentally different from traditional closed containers," and analogizes them to "homes" and the "human mind." Arnold's analogy of a laptop to a home is based on his conclusion that a laptop's capacity allows for the storage of personal documents in an amount equivalent to that stored in one's home. He argues that a laptop is like the "human mind" because of its ability to record ideas, e-mail, internet chats and web-surfing habits.

Lastly, Arnold argues that application of First Amendment principles requires us to rule contrary to the Fourth Circuit in *United States v. Ickes*, 393 F.3d 501, 506-08 (4th Cir. 2005) (rejecting the argument based on the First Amendment that a higher level of suspicion is needed for searches of "expressive material"), and to promulgate a reasonable suspicion requirement for border searches where the risk is high that expressive material will be exposed.

III

A

[1] The Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. Const. amend. IV. Searches of international passengers at American airports are considered border searches because they occur at the "functional equivalent of a border." *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973) ("For . . . example, a search of the passengers and

cargo of an airplane arriving at a St. Louis airport after a non-stop flight from Mexico City would clearly be the functional equivalent of a border search."). "It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). Generally, "searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border . . . ." *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

[2] The Supreme Court has stated that:

> The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity. By reason of that authority, it is entitled to require that whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry.

Torres v. Puerto Rico, 442 U.S. 465, 472-73 (1979). In other words, the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152. Therefore, "[t]he luggage carried by a traveler entering the country may be searched at random by a customs officer . . . no matter how great the traveler's desire to conceal the contents may be." *United States v. Ross*, 456 U.S. 798, 823 (1982). Furthermore, "a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf [may] claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case." *Id.* at 822.

B

[3] Courts have long held that searches of closed containers and their contents can be conducted at the border without par-

ticularized suspicion under the Fourth Amendment. Searches of the following specific items have been upheld without particularized suspicion: (1) the contents of a traveler's briefcase and luggage, *United States v. Tsai*, 282 F.3d 690, 696 (9th Cir. 2002); (2) a traveler's "purse, wallet, or pockets," *Henderson v. United States*, 390 F.2d 805, 808 (9th Cir. 1967); (3) papers found in containers such as pockets, see *United States v. Grayson*, 597 F.2d 1225, 1228-29 (9th Cir. 1979) (allowing search without particularized suspicion of papers found in a shirt pocket); and (4) pictures, films and other graphic materials. *See United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971); *see also 12,200-Ft. Reels of Super 8MM. Film*, 413 U.S. 123, 124-25 (1973) ("Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations.").

Nevertheless, the Supreme Court has drawn some limits on the border search power. Specifically, the Supreme Court has held that reasonable suspicion is required to search a traveler's "alimentary canal," *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985), because " '[t]he interests in human dignity and privacy which the Fourth Amendment protects forbid any such intrusion [beyond the body's surface] on the mere chance that desired evidence might be obtained.' " *Id.* at 540 n.3 (quoting *Schmerber v. California*, 384 U.S. 757, 769 (1966)). However, it has expressly declined to decide "what level of suspicion, *if any*, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches." *Id.* at 541 n.4 (emphasis added). Furthermore, the Supreme Court has rejected creating a balancing test based on a "routine" and "nonroutine" search framework, and has treated the terms as purely descriptive. *See United States v. Cortez-Rocha*, 394 F.3d 1115, 1122 (9th Cir. 2005).

[4] Other than when "intrusive searches of *the person*" are at issue, *Flores-Montano*, 541 U.S. at 152 (emphasis added),

the Supreme Court has held open the possibility, "that some searches of *property* are so destructive as to require" particularized suspicion. *Id.* at 155-56 (emphasis added) (holding that complete disassembly and reassembly of a car gas tank did not require particularized suspicion). Indeed, the Supreme Court has left open the question of " 'whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out.' " *Id.* at 155 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13).

C

In any event, the district court's holding that particularized suspicion is required to search a laptop, based on cases involving the search of the person, was erroneous. Its reliance on such cases as *United States v. Vance*, 62 F.3d 1152, 1156 (9th Cir. 1995) (holding that "[a]s the search becomes more intrusive, more suspicion is needed" in the context of a search of the human body), to support its use of a sliding intrusiveness scale to determine when reasonable suspicion is needed to search property at the border is misplaced. *United States v. Arnold*, 454 F. Supp. 2d 999, 1002-04 (C.D. Cal. 2006).

[5] The Supreme Court has stated that "[c]omplex balancing tests to determine what is a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person, have no place in border searches of vehicles." *Flores-Montano*, 541 U.S. at 152. Arnold argues that the district court was correct to apply an intrusiveness analysis to a laptop search despite the Supreme Court's holding in *Flores-Montano*, by distinguishing between one's privacy interest in a vehicle compared to a laptop. However, this attempt to distinguish *Flores-Montano* is off the mark. The Supreme Court's analysis determining what protection to give a vehicle was not based on the unique characteristics of vehicles with respect to other property, but was based on the fact that a vehicle, as a piece of property, simply does not implicate the same "dignity and pri-

vacy" concerns as "highly intrusive searches of the person." *Flores-Montano*, 541 U.S. at 152.

[6] Furthermore, we have expressly repudiated this type of "least restrictive means test" in the border search context. *See Cortez-Rocha*, 394 F.3d at 1123 (refusing to fashion a "least restrictive means test for border control vehicular searches, and . . . refus[ing] to tie the hands of border control inspectors in such a fashion"). Moreover, in both *United States v. Chaudhry*, 424 F.3d 1051, 1054 (9th Cir. 2005) (finding the distinction between "routine" and "non-routine" inapplicable to searches of property) and *Cortez-Rocha*, 394 F.3d at 1122-23, we have recognized that *Flores-Montano* rejected our prior approach of using an intrusiveness analysis to determine the reasonableness of property searches at the international border.

[7] Therefore, we are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.[1]

IV

While the Supreme Court left open the possibility of requiring reasonable suspicion for certain border searches of property in *Flores-Montano*, 541 U.S. at 155-56, the district court did not base its holding on the two narrow grounds left open by the Supreme Court in that case.

Arnold has never claimed that the government's search of his laptop damaged it in any way; therefore, we need not con-

[1]We recently issued an opinion on a separate issue of whether reasonable suspicion is required to search outgoing international correspondence; however, this opinion has since been withdrawn and the case has been reheard by an en banc panel of this court that has yet to issue a decision. *United States v. Seljan*, 497 F.3d 1035 (9th Cir. 2007), *withdrawn by* 512 F.3d 1203 (9th Cir. 2008) (ordering rehearing en banc).

sider whether "exceptional damage to property" applies. Arnold does raise the "particularly offensive manner" exception to the government's broad border search powers.[2] But, there is nothing in the record to indicate that the manner in which the CBP officers conducted the search was "particularly offensive" in comparison with other lawful border searches. According to Arnold, the CBP officers simply "had me boot [the laptop] up, and looked at what I had inside . . . ."

[8] Whatever "particularly offensive manner" might mean, this search certainly does not meet that test. Arnold has failed to distinguish how the search of his laptop and its electronic contents is logically any different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed. *See Ross*, 456 U.S. at 823; *see also Vance*, 62 F.3d at 1156 ("In a border search, a person is subject to search of luggage, contents of pockets and purse without any suspicion at all.").

[9] With respect to these searches, the Supreme Court has refused to draw distinctions between containers of information and contraband with respect to their quality or nature for purposes of determining the appropriate level of Fourth Amendment protection. Arnold's analogy to a search of a home based on a laptop's storage capacity is without merit. The Supreme Court has expressly rejected applying the

[2]Notwithstanding the government's objection, we can decide this issue because the "particularly offensive manner" exception can be found in *Flores-Montano*, which was presented to the district court by the parties, and "the matter [of what the Fourth Amendment requires] was fairly before the [district court]" and, in any event, it is a question of law. *See Nelson v. Adams USA, Inc.*, 529 U.S. 460, 469-70 (2000); *see also Ballaris v. Wacker Siltronic Corp.*, 370 F.3d 901, 908 (9th Cir. 2004) ("Once a federal claim is properly presented, a party can make any argument in support of that claim; parties are not limited to the precise argument they made below. . . . Where . . . the question presented is one of law, we consider it in light of all relevant authority, regardless of whether such authority was properly presented in the district court." (citations and quotation marks omitted)).

Fourth Amendment protections afforded to homes to property which is "*capable of functioning as a home*" simply due to its size, or, distinguishing between " 'worthy and 'unworthy' containers." *California v. Carney*, 471 U.S. 386, 393-94 (1985).

In *Carney*, the Supreme Court rejected the argument that evidence obtained from a warrantless search of a mobile home should be suppressed because it was "*capable of functioning as a home*." *Id*. at 387-88, 393-94. The Supreme Court refused to treat a mobile home differently from other vehicles just because it could be used as a home. *Id.* at 394-95. The two main reasons that the Court gave in support of its holding, were: (1) that a mobile home is "readily movable," and (2) that "the expectation [of privacy] with respect to one's automobile is significantly less than that relating to one's home or office." *Id.* at 391 (quotation marks omitted).

[10] Here, beyond the simple fact that one cannot live in a laptop, *Carney* militates against the proposition that a laptop is a home. First, as Arnold himself admits, a laptop goes with the person, and, therefore is "readily mobile." *Carney*, 471 U.S. at 391. Second, one's "expectation of privacy [at the border] . . . is significantly less than that relating to one's home or office." *Id.*

Moreover, case law does not support a finding that a search which occurs in an otherwise ordinary manner, is "particularly offensive" simply due to the storage capacity of the object being searched. *See California v. Acevedo*, 500 U.S. 565, 576 (1991) (refusing to find that "looking inside a closed container" when already properly searching a car was unreasonable when the Court had previously found "destroying the interior of an automobile" to be reasonable in *Carroll v. United States*, 267 U.S. 132 (1925)).

[11] Because there is no basis in the record to support the contention that the manner in which the search occurred was

"particularly offensive" in light of other searches allowed by the Supreme Court and our precedents, the district court's judgment cannot be sustained.

V

Finally, despite Arnold's arguments to the contrary we are unpersuaded that we should create a split with the Fourth Circuit's decision in *Ickes*. In that case, the defendant was stopped by Customs agents as he attempted to drive his van from Canada into the United States. 393 F.3d at 502. Upon a "cursory search" of defendant's van, the inspecting agent discovered a video camera containing a tape of a tennis match which "focused excessively on a young ball boy." *Id*. This prompted a more thorough examination of the vehicle, which uncovered several photograph albums depicting provocatively-posed prepubescent boys, most nude or semi-nude. *Id.* at 503.

The Fourth Circuit held that the warrantless search of defendant's van was permissible under the border search doctrine. The court refused to carve out a First Amendment exception to that doctrine because such a rule would: (1) protect terrorist communications "which are inherently 'expressive' "; (2) create an unworkable standard for government agents who "would have to decide—on their feet—which expressive material is covered by the First Amendment"; and (3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First Amendment interest is also at stake. *See id.* at 506-08 (citing *New York v. P.J. Video*, 475 U.S. 868, 874 (1986) (refusing to require a higher standard of probable cause for warrant applications when expressive material is involved)).

We are persuaded by the analysis of our sister circuit and will follow the reasoning of *Ickes* in this case.

VI

For the foregoing reasons, the district court's decision to grant Arnold's motion to suppress must be

REVERSED.

Taking your laptop into the US? Be sure to hide all your data first

Bruce Schneier

The Guardian, Thursday 15 May 2008

http://www.guardian.co.uk/technology/2008/may/15/computing.security

Stolen Laptop Helps Turn Tables on Suspects

By LISA W. FODERARO
Published: May 10, 2008

http://www.nytimes.com/2008/05/10/nyregion/10laptop.html?_r=1&oref=slogin

$20 Million Settlement Reached for Veterans in ID Theft Suit

By THE ASSOCIATED PRESS
Published: January 27, 2009

http://www.nytimes.com/2009/01/28/washington/28vets.html

For Release: February 18, 2009

CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations

MEDIA CONTACT:

Claudia Bourne Farrell,
Office of Public Affairs
202-326-2181

STAFF CONTACT:

Alain Sheer,
Bureau of Consumer Protection
202-326-2252

Loretta Garrison,
Bureau of Consumer Protection
202-326-2252

(FTC File No. 072 3119)
(cvs)

http://www.ftc.gov/opa/2009/02/cvs.shtm

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of
CVS CAREMARK CORPORATION, a corporation,

Complaint

http://www.ftc.gov/os/caselist/0723119/090218cvscmpt.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of
CVS CAREMARK CORPORATION, a corporation,

Complaint: Exhibit A

http://www.ftc.gov/os/caselist/0723119/090218cvscmptexha.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of
CVS CAREMARK CORPORATION, a corporation,

AGREEMENT CONTAINING CONSENT ORDER

http://www.ftc.gov/os/caselist/0723119/090218cvsagree.pdf

Analysis of Proposed Consent Order to Aid Public Comment

In the Matter of CVS Caremark Corporation, File No. 0723119

http://www.ftc.gov/os/caselist/0723119/090218cvsanal.pdf

For Release: November 6, 2008

Mortgage Company Settles Data Security Charges

Data Breach Compromised Privacy of Hundreds of Consumers

MEDIA CONTACT:

Betsy Lordan,
Office of Public Affairs
202-326-3707

STAFF CONTACT:

Jessica Rich,
Bureau of Consumer Protection
202-326-2148

(FTC File No. 0723004)
(PCL.final.wpd)

http://www.ftc.gov/opa/2008/11/pcl.shtm

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of PREMIER CAPITAL LENDING, INC. a corporation; and DEBRA STILES, individually and as an officer of the corporation.

Complaint

http://www.ftc.gov/os/caselist/0723004/081206pclcmpt.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of PREMIER CAPITAL LENDING, INC. a corporation; and DEBRA STILES, individually and as an officer of the corporation.

Decision and Order

http://www.ftc.gov/os/caselist/0723004/081216pcldo.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of PREMIER CAPITAL LENDING, INC. a corporation; and DEBRA STILES, individually and as an officer of the corporation.

Agreement Containing Consent Order

http://www.ftc.gov/os/caselist/0723004/081106pclagree.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of PREMIER CAPITAL LENDING, INC. a corporation; and DEBRA STILES, individually and as an officer of the corporation.

Analysis of Proposed Consent Order to Aid Public Comment

http://www.ftc.gov/os/caselist/0723004/081106pclagree.pdf

FSA fines stockbroker Merchant Securities for slack security

18 June 2008 - 10:10

http://www.finextra.com/fullstory.asp?id=18599

London FSA Matter

13 June 2008

Summary: The Financial Services Authority of 25 The North Colonnade, Canary Wharf, London E14 5HS (the FSA) gives you final notice about a requirement to pay a financial penalty.

http://www.fsa.gov.uk/pubs/final/merchant_13jun08.pdf

Stockbroking firm fined £77,000 for weak Data Security Controls

17 June 2008

http://www.fsa.gov.uk/pages/Library/Communication/PR/2008/058.shtml

Cost of a Security Breach

Friday, April 13, 2007

http://securityspace.blogspot.com/2007/04/cost-of-security-breach.html

The Real Cost of a Security Breach

David Hobson, Managing Director of Global Gecure Systems

August 12, 2008

http://www.scmagazineus.com/The-real-cost-of-a-security-breach/article/113717/

Security 101: Cost of a Breach

http://www.secureworks.com/research/newsletter/2007/10/

Fannie Mae Logic Bomb Would Have Caused Weeklong Shutdown

By Kevin Poulsen | January 29, 2009 | 1:41:19 PM | Categories: Threats

http://blog.wired.com/27bstroke6/2009/01/fannie.html

Fannie Mae Logic Bomb Makes Case For Strong IDM

Posted by: **George Hulme, Jan 29, 2009 09:27 PM**

http://www.informationweek.com/blog/main/archives/2009/01/fannie_mae_logi.html

FTC questions cloud-computing security

By Stephanie Condon
March 17, 2009 6:30 PM PDT

http://news.cnet.com/8301-13578_3-10198577-38.html

Privacy & Security Task Force ADVISORY

States Adopting Aggressive New Privacy and Data Security Laws and Regulations

October 7, 2008

http://www.alston.com/files/Publication/05c1737d-ccfc-44a2-9252-1ffbea8953d3/Presentation/PublicationAttachment/a5a0be6c-e8c5-4b3c-ad17-134c3b6f0cd6/Privacy%20Post%20Vol%204.pdf

If you would like to receive future *Privacy & Security Task Force Advisories* electronically, please forward your contact information including e-mail address to **Privacy.Post@alston.com.** Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of our **Privacy & Security Task Force** attorneys.

201 CMR 17.00:
Standards for The Protection of Personal Information of Residents of the Commonwealth

http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=reg201cmr17&csid=Eoca

SB 20 Senate Bill Analysis
Senate Judiciary Commitee
Senator Ellen M. Corbett, Chair
2009-2010 Regular Session

http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_20_cfa_20090224_164247_sen_comm.html

AMENDED IN SENATE MARCH 4, 2009

SENATE BILL No. 20

Introduced by Senator Simitian

December 1, 2008

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 20, as amended, Simitian. Personal information: privacy.

Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would require any agency, person, or business that must issue a security breach notification pursuant to existing law to fulfill certain additional requirements pertaining to the security breach notification, as specified.

The bill would also require any agency, person, or business that must issue a security breach notification to more than 500 California residents pursuant to existing law to electronically submit that security breach notification to the Attorney General.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that must issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information~~, as defined in subdivision (g),~~ that were or are reasonably believed to have been the subject of a breach.

(C) The date, estimated date, or date range within which the breach occurred, if that information is possible to determine at the time the notice is provided, and the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation.

(E) A general description of the breach incident.

(F) The estimated number of persons affected by the breach.

(G) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a bank account or credit card number, a social security number, or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that must issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit that security breach notification to the Attorney General.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully

made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security and Privacy Protection.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 2. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the

security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any person or business that must issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information~~, as defined in subdivision (g),~~ that were or are reasonably believed to have been the subject of a breach.

(C) The date, or estimated date, or date range within which the breach occurred, if that information is possible to determine at the time the notice is provided, and the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation.

(E) A general description of the breach incident.

(F) The estimated number of persons affected by the breach.

(G) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a bank account or credit card number, a social security number, or a driver's license or California identification card number.

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any person or business that must issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit that security breach notification to the Attorney General.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media and the Office of Information Security and Privacy Protection.

(j) Notwithstanding subdivision (i), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

O

Annotated Internet Links: Global Data Security and Privacy

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF
December 27, 2001, European Commission Decision with recommended clauses for transfer of data to third parties outside of the EEA ("European Economic Area" including EU member countries and other countries implementing the Directive of October 24, 1995).

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
European Commission home page for data protection resources.

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm
European Commission list of European, US, and Asian Data Protection Commissioners and privacy officers.

http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm
European Commission page with multiple resources relating to model contracts for transfer of data to non-EU countries.

http://useu.usmission.gov/Dossiers/Data_Privacy/default.asp
Main Data Privacy page of the US Mission to the European Union.

http://useu.usmission.gov/Dossiers/Data_Privacy/Dec1208_SLCG_Statement.asp\
December 12, 2008, US, EU Issue Statement on Common Data Privacy and Protection Principles (focused on anti-terrorism and law enforcement issues)

http://ftc.gov/privacy/
FTC Main page for privacy initiatives, including news of enforcement actions, and information on deception (misleading consumers re privacy practices), financial privacy, credit reporting and children's privacy.

http://www.ftc.gov/infosecurity/
FTC interactive guide for businesses on protecting personal information.

http://www.export.gov/safeharbor/
US Department of Commerce site on "Safe Harbor" for data protection/privacy transactions with European countries.

http://www.export.gov/safeharbor/SH_Overview.asp
Safe Harbor Overview including list of key Safe Harbor principles

http://www.export.gov/safeharbor/Sh_Checklist.asp
Safe Harbor checklist

http://www.export.gov/safeharbor/SH_Documents.asp
Comprehensive set of Safe Harbor documents (including critical FAQs)

http://export.gov/safeharbor/SH_Helpful_Hints.asp
Helpful Hints for a Safe Harbor policy and compliance

http://export.gov/safeharbor/SH_Privacy_Links.asp
Data Privacy links and further resources

http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list
US Department of Commerce list of organizations representing that they have complied with safe harbor policy framework.

http://infotech.aicpa.org/Resources/Systems+Audit+and+Internal+Control/IT+Systems+Audit/Standards+and+Regulations/SAS+No.+70+Service+Organizations.htm
AICPA resource page for auditors' guidelines on SAS 70

http://infotech.aicpa.org/Resources/Privacy/
AICPA privacy resource page (note that beta "privacy tool" is available only to members of AICPA but may be requested by others).

http://infotech.aicpa.org/Resources/Privacy/
AICPA privacy resource page (note that beta "privacy tool" is available only to members of AICPA but may be requested by others).

http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/national_laws/2NATIONAlLAWS_en.asp#TopOfPage
Council of Europe matrix of National Laws on privacy and data protection for European member countries, non-member countries and North America, South America, Asia.

http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html
OECD (Organisation for Economic Co-Operation and Development) Privacy Policy Generator, including guidelines and an interactive policy generator.

http://www.oecd.org/document/1/0,3343,en_2649_34255_28863233_1_1_1_1,00.html
OECD "How to Develop a Privacy Policy" with checklist of questions

http://www2.oecd.org/pwv3/
OECD interactive policy statement generator questionnaire (need to register to begin).

http://www.dmaresponsibility.org/InfoSecurity/
Direct Marketing Association checklist for information security practices.

For an electronic copy the hyperlinks above, please e-mail your request to: jonathan.gordon@alston.com

Where Did That Content Come From?

Implications of Promotional Marketing User-Generated Content and Online Behavioral Targeting

Katherine Wallace
March 31, 2009

Engaging the Consumer

Common Messages From the Marketing Team:

- We want to engage the consumer where the consumer is.
- We want to drive traffic to the site.
- We want the site to be edgy and sticky.
- We want the consumer to have “fun” interacting with the site.
- We want to get better distribution through viral means.
- The functionality is available, and we want to use it.

Where Do They Want to Engage?

BLOGS

SOCIAL NETWORKING SITES

TWITTER

WIDGETS

RSS FEEDS

PRODUCT PLACEMENT

ONLINE INTEGRATED MARKETING

Let's Set the Stage

New Website for Launch of New Product

- Website will have blog/comments features and RSS Feeds.
- Website will have functionality to allows users to develop and post content and send that content to a friend.
  - Functionality to create short song and include text/lyrics
  - Functionality to upload picture or image into a static scene
  - Functionality to tag/modify a website and capture the screen image
- Website will have functionality to allow users to submit ideas for new applications/features for the website.

AND . . .

Contest Promotion to Coincide with Product Launch

- Consumers (18 and older) in the US are to submit a video with proposed idea for a commercial for the company's new product. Entrants are encouraged to make prominent use of the company's brand in the video entry.
- Entries are to be submitted to the company website, where they will be posted for judging and comment by website users as public rating is an element of the judging criteria.
- To help encourage their friends to visit the website to vote for their entry, entrants are encouraged and provided functionality to submit their videos for posting on their Facebook pages.
- Winning entry will become the basis for new advertising campaign in print, on television, radio and internet.
- Winner receives trip for winner and friend to Las Vegas for a few nights to attend party, photo shoots, etc. in connection with launch of the product and winner is to use Twitter to keep fans of the site posted regarding the events.

Areas Of Concern

- Major Areas of Legal Risk and Concern
  - Intellectual Property Concerns
    - Copyright infringement
    - Trademark infringement
    - Idea misappropriation
  - Rights of Publicity / Privacy Issues
  - COPPA
  - Defamation, Libel and Slander
  - False Advertising / Unfair Competition
  - Tort Liability
  - State Law Claims

What Legal Protections Are There?

- Digital Millennium Copyright Act
- Communications Decency Act
- Affirmative Defenses for Copyright Infringement
- Fair Use Defenses
- Terms and Conditions

ALSTON+BIRD LLP

Steps to Help Mitigate the Risk

- **Determine up front how you want to use the content that you receive.**
- **Determine up front limitations on who is able to participate.**
- **It's OK to be conservative.**
  - Provide for specific and comprehensive terms and conditions and official rules to which users/entrants must affirmatively agree.
  - Consider making certain functionality available only to registered users of the site.
  - Consider obtaining written releases and consents up front.
  - Implement monitoring, filtering and screening procedures.
  - Use disclaimers and notices, as appropriate.
  - Provide "neutral tools" and pre-cleared content for use with tools on the site.
- **Be in a position to take advantage of the laws that protect you.**
- **Confirm terms of use for other sites to be used in connection with the promotion.**

ALSTON+BIRD LLP

So . . . . How Else Can We Engage the Consumer?

Target your content and advertising to their interests

Online Behavioral Targeting

- **What is it?**
  - Practice of tracking an individual's online activities *over time* in order to deliver advertising tailored to his or her interests
  - Implemented through means such as "persistent" cookies and network advertising

Examples

- **Example #1** – Browser-Based Marketing - Consumer visits a website regarding automobiles and conducts a search for sports cars and specific manufacturers. Consumer does not purchase a car or contact a dealer, but later visits a local news website. On the news website, the consumer is shown an advertisement for a sports car from a particular manufacturer.
- **Example #2** – Location Based Marketing – Implemented through location aware devices, such as wireless devices with GPS. Consumer is vacationing in Los Angeles for the first time. At the hotel room, he pulls out his wireless device, logs onto the web and searches for "Thai restaurants in Los Angeles." Fifty results come back. So he clicks the "location-based" feature on the device which triggers a GPS satellite feed to pinpoint his exact location within the city. Now only three restaurants, relevant to his physical location show up in the search results based on coding data implemented in the web site.

ALSTON+BIRD LLP

Current Regulatory Framework

- ***Primarily*** **Self Regulation**
  - **NAI (Network Advertising Initiative)**
  - **Mobile Marketing Association**
  - **CTIA-The Wireless Association**
  - **Certification processes (e.g. TRUSTe)**
  - **Marketing and Trade Associations (DMA, IAB, BBB)**
  - **Individual Advertising Network policies**
  - **Privacy Statements and Practices**
- **FTC has published revised Self-Regulatory Principles for Online Behavioral Advertising**
- **Goals of Self-Regulation**
  - *FTC's guidance - "Address practices that raise genuine privacy concerns without interfering with practices – or stifling innovation – where privacy concerns are minimal."*

ALSTON+BIRD LLP

Can Self-Regulation Work?

- Lessons of history
- Challenges of enforcement
- Need for consumer education
- Free-Riders
- Is the “industry” aligned with same goals?

Therein lies the challenge for the industry, the lawyers and the policy professionals . . . .

ALSTON+BIRD LLP

Who Changed My Backend?

Issues raised by the continued adoption of cloud computing and open source

David S. Teske
March 31, 2009

Jacobsen v. Katzer

- *Jacobsen v. Katzer*, *87 USPQ2d 1836* (Fed. Cir. 2008)
- Facts: The defendants copied portions of plaintiff's open source JMRI software. Defendants incorporated these portions into their commercial software without following the terms of the plaintiff's open source license.
- Claim: Plaintiff brought suit for *copyright infringement* in federal district court in California and moved for a preliminary injunction.

Jacobsen v. Katzer

Issue:

- **Note: Generally a "copyright owner who grants a nonexlusive license to use his copyrighted material waives his right to sue the licensee for copyright infringement" unless the license is "limited in scope" and "the licensee acts outside the scope."**
- High level: Whether the defendant was outside the scope of the license (copyright infringement) or within the scope of the license (breach of contract).
- Lower level: Whether the terms of the open source Artistic License were **conditions** on the scope of the license (allowing a theory of copyright infringement), or whether the terms of the Artistic License were merely **covenants** that impose obligations without affecting the scope of the license, (allowing only a suit under a breach of contract theory).

Jacobsen v. Katzer

Plaintiff Argument:

- The defendant modified the software without following the conditions and thus exceeded the scope of the license.

Defendant Argument:

- Failure to insert a prominent notice of attribution is not an act that exceeds the scope of the license; rather the violation was merely a violation of a *covenant*, allowing a cause of action under contract, but not copyright infringement.
- Defendants admit copyright infringement; but argue a defense to such a claim based on their license to use the material.
- Neither economic damages nor injunctive relief are appropriate

Jacobsen v. Katzer

Lower Court Ruling (for defendants):

- The district court denied the plaintiff's request for injunction saying that the "defendants' alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license, but does not create liability for copyright infringement."

Jacobsen v. Katzer

CAFC Ruling (for plaintiff):

- The appellate court vacated the lower court's ruling and remanded holding the attribution requirements **created conditions on the scope of the copyright license.**
- "Under California contract law, 'provided that' typically denotes a condition."
- The introduction of the Artistic License states "The intent of this document is to state the **conditions** under which a Package may be copied"

Jacobsen v. Katzer

- GPL –
  - All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met.
  - You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you…
  - You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions
- Apache 2.0 -
  - You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions

Jacobsen v. Katzer

- CAFC:

  Traditionally, copyright owners sold their copyrighted material in exchange for money. The lack of money changing hands in open source licensing should not be presumed to mean that there is no economic consideration, however. There are substantial benefits, including economic benefits, to the creation and distribution of copyrighted works under public licenses that range far beyond traditional license royalties. For example, program creators may generate market share for their programs by providing certain components free of charge. Similarly, a programmer or company may increase its national or international reputation by incubating open source projects.

Jacobsen v. Katzer

- CAFC:

  Copyright licenses are designed to support the right to exclude; money damages alone do not support or enforce that right. The choice to exact consideration in the form of compliance with the open source requirements of disclosure and explanation of changes, rather than as a dollar-denominated fee, is entitled to no less legal recognition. Indeed, because a calculation of damages is inherently speculative, these types of license restrictions might well be rendered meaningless absent the ability to enforce through injunctive relief.

Jacobsen v. Katzer Part II

Jacobsen v. Katzer, 89 USPQ2d 1441 (N.D. Cal. 2009)

- District Court accepts that
  - copyright infringement may occur
  - preliminary injunction is an available remedy
- But requires proof to meet a heightened burden of demonstrated harm

Jacobsen v. Katzer Part II

- A plaintiff is not granted the presumption of irreparable harm upon a showing of likelihood of success on the merits. Instead, a plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.

Jacobsen v. Katzer Part II

- Court acknowledges various *possible* harms listed by the CAFC.
- Does not find any proof of harm presented by the plaintiff
- But:
  - Even if Jacobsen's heavy burden to warrant injunctive relief had been met, it is unclear how the Court would fashion an injunction which would be narrowly tailored to enjoin only those allegedly infringing uses of Jacobsen's copyrighted content.

Jacobsen v. Katzer

Take Away:

- Technical violations of open source licenses may give rise to copyright infringement and can support monetary damages and preliminary injunction.
- Preliminary injunction must be supported by harm that is real, imminent and significant, not just speculative or potential
  - What would the injunction look like?
- Permissive License (e.g. BSD, MIT and Artistic)
  - Without copyright registration, limited (if any) monetary damages
  - Scope of injunction limited to future compliance?
- Restrictive License (e.g. GPL and LGPL)
  - Without copyright registration, limited (if any) monetary damages
  - Scope of injunction to force disclosure of combined works

Microsoft v. TomTom N.V.

- Microsoft alleges eight patents infringed by TomTom navigation devices
  - 5 related to car navigation
  - 3 related to file management
- 5,579,517 – Common Name Space for Long and Short Filenames

Microsoft v. TomTom N.V.

- Is this the beginning of an offensive against Linux?
- Horacio Gutierrez of Microsoft
  - "(It's the) TomTom implementation of the Linux kernel that infringes these claims. There are many flavors of Linux (and) many implementations of the Linux kernel. Cases such as these are very fact-specific. . . . This is just a normal course-of-business dispute between two companies. (Linux) is not the focal point of the action. "

Microsoft v. TomTom N.V.

- TomTom joined the Open Invention Network (OIN)
- OIN goal is to promote Linux
- Linux Defenders
  - Software Freedom Law Center
  - Linux Foundation

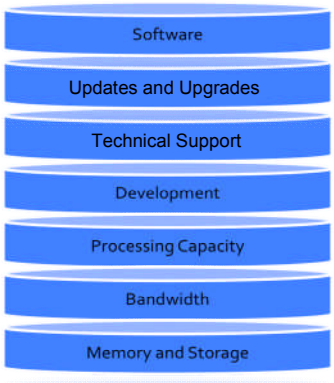
Who Changed My Backend?

Issues raised by the continued adoption of cloud computing and open source

Todd McClelland
March 31, 2009
Los Angeles, CA

ALSTON+BIRD LLP

Your Data Center



Security

Power & Cooling

ALSTON+BIRD LLP

Data Center Hassles

- Constantly negotiating software contracts with always changing price structures
- Updating one applications affects multiple applications. Vista!
- 55% of capacity goes unused most of the time
- Increasingly complex systems makes security a nightmare
- Big up-front costs, a substantial investment
- New technology requires new subject matter experts
- Technology rapidly goes out of date
- Difficult to scale up

The New Paradigm: Cloud Computing

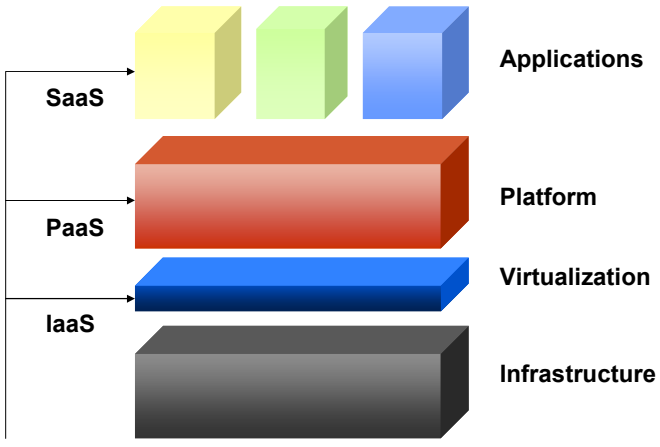
"Cloud computing represents a new way to deploy computing technology to give users the ability to access, work on, share, and store information using the Internet. The cloud itself is a network of data centers – each composed of many thousands of computers working together – that can perform the functions of software on a personal or business computer by providing users access to powerful applications, platforms, and services delivered over the Internet."

Jeffrey F. Rayport and Andrew Heyward: "Envisioning the Cloud: The Next Computing Paradigm," March 20, 2009.

Three Typical Structures

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Variations of Cloud Services



Selling Points

- Scalable to your needs
- Pay as you go utility pricing (bandwidth, server usage, storage)
- Cost predictability
- Access to expertise
- Redundancy, Reliability, Flexibility
- Access to a platform to develop, test, deploy, host and maintain applications
- Lower capital cost and less time to get up and running
- Focus on development and core business

Examples

- Google Maps; Google Docs; Flickr; YouTube
- salesforce.com
- Facebook; MySpace
- Second Life
- WorldofWarcraft
- LexisNexis; Westlaw
- Amazon EC2 (Elastic Compute Cloud)
- Amazon S3 (Simple Storage Service)
- Yahoo! Reasearch
- Microsoft Azure
- Wikipedia

Cloud Computing Concerns

- Security
- Privacy
- Reliability
- Exposure
- Exit Strategy
- Contract Terms

Security

- Single biggest concern of everyone using cloud computing
- Might be safer (e.g., Patches)
- Data is typically NOT physically segregated
- Look at the Vendor's policy
- Audit rights? Verification?
- Standards?
- PCI? HIPAA? EU Data Directive?

Privacy

- Where is your data now? Where will it be?
- Government Access
- Use by the Vendor (e.g., Targeted ads in emails)
- Reconciling legal requirements
- Patriot Act

Reliability

- Vendor suspension rights
- SLAs
- Bankruptcy
- Governmental actions
- Disasters
- Software/Hardware failures

Exposure

- New Government/legal regime exposure
- Breach (Trade Secret, notification issues, etc.)
- Data location
- Import/Export control
- IP
- Compliance with laws (Can I do this?)
- Pricing (Bursting)
- Contractual
- Disaster Recovery/ Business Continuity

Exit Strategy

- Separation “prenup”
- Return of data, no matter what
  - Include desired format and right to data maps
- Rights to terminate
- Vendor’s right to terminate?
- How long will it take to transition?
- Termination fees? What is the total cost to terminate?
- Termination assistance?
- Transition assistance?

Common Contract Terms

- "Outsourcing Light"
- Acceptable Use Policy
- Pricing
- SLAs
- Verification/Audit rights?
- Suspension rights
- IP
- Privacy/Security
- Breaches
- Limitations on liability/ Indemnification
- Disaster Recovery

ALSTON+BIRD LLP

Supporting Materials

United States Court of Appeals for the Federal Circuit

2008-1001

ROBERT JACOBSEN,

Plaintiff-Appellant,

v.

MATTHEW KATZER and
KAMIND ASSOCIATES, INC. (doing business as KAM Industries),

Defendants-Appellees.

Victoria K. Hall, Law Office of Victoria K. Hall, of Bethesda, Maryland, argued for plaintiff-appellant.

R. Scott Jerger, Field Jerger LLP, of Portland, Oregon, argued for defendants-appellees.

Anthony T. Falzone, Stanford Law School, Center for Internet and Society, of Stanford, California, for amici curiae Creative Commons Corporation, et al. With him on the brief was Christopher K. Ridder.

Appealed from: United States District Court for the Northern District of California

Judge Jeffrey S. White

United States Court of Appeals for the Federal Circuit

2008-1001

ROBERT JACOBSEN,

Plaintiff-Appellant,

v.

MATTHEW KATZER and
KAMIND ASSOCIATES, INC. (doing business as KAM Industries),

Defendants-Appellees.

Appeal from the United States District Court for the Northern District of California in case no. 06-CV-1905, Judge Jeffrey S. White.

DECIDED: August 13, 2008

Before MICHEL, Chief Judge, PROST, Circuit Judge, and HOCHBERG,[*] District Judge.

HOCHBERG, District Judge.

We consider here the ability of a copyright holder to dedicate certain work to free public use and yet enforce an "open source" copyright license to control the future distribution and modification of that work. Appellant Robert Jacobsen ("Jacobsen") appeals from an order denying a motion for preliminary injunction. Jacobsen v. Katzer, No. 06-CV-01905 JSW, 2007 WL 2358628 (N.D. Cal. Aug. 17, 2007). Jacobsen holds a copyright to computer programming code. He makes that code available for public download from a

[*] The Honorable Faith S. Hochberg, District Judge, United States District Court for the District of New Jersey, sitting by designation.

website without a financial fee pursuant to the Artistic License, an "open source" or public license. Appellees Matthew Katzer and Kamind Associates, Inc. (collectively "Katzer/Kamind") develop commercial software products for the model train industry and hobbyists. Jacobsen accused Katzer/Kamind of copying certain materials from Jacobsen's website and incorporating them into one of Katzer/Kamind's software packages without following the terms of the Artistic License. Jacobsen brought an action for copyright infringement and moved for a preliminary injunction.

The District Court held that the open source Artistic License created an "intentionally broad" nonexclusive license which was unlimited in scope and thus did not create liability for copyright infringement. The District Court reasoned:

> The plaintiff claimed that by modifying the software the defendant had exceeded the scope of the license and therefore infringed the copyright. Here, however, the JMRI Project license provides that a user may copy the files verbatim or may otherwise modify the material in any way, including as part of a larger, possibly commercial software distribution. The license explicitly gives the users of the material, any member of the public, "the right to use and distribute the [material] in a more-or-less customary fashion, plus the right to make reasonable accommodations." The scope of the nonexclusive license is, therefore, intentionally broad. The condition that the user insert a prominent notice of attribution does not limit the scope of the license. Rather, Defendants' alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license, but does not create liability for copyright infringement where it would not otherwise exist.

Jacobsen, 2007 WL 2358628 at *7 (internal citations omitted).

On this basis, the District Court denied the motion for a preliminary injunction. We vacate and remand.

I.

Jacobsen manages an open source software group called Java Model Railroad Interface ("JMRI"). Through the collective work of many participants, JMRI created a

computer programming application called DecoderPro, which allows model railroad enthusiasts to use their computers to program the decoder chips that control model trains. DecoderPro files are available for download and use by the public free of charge from an open source incubator website called SourceForge; Jacobsen maintains the JMRI site on SourceForge. The downloadable files contain copyright notices and refer the user to a "COPYING" file, which clearly sets forth the terms of the Artistic License.

Katzer/Kamind offers a competing software product, Decoder Commander, which is also used to program decoder chips. During development of Decoder Commander, one of Katzer/Kamind's predecessors or employees is alleged to have downloaded the decoder definition files from DecoderPro and used portions of these files as part of the Decoder Commander software. The Decoder Commander software files that used DecoderPro definition files did not comply with the terms of the Artistic License. Specifically, the Decoder Commander software did not include (1) the authors' names, (2) JMRI copyright notices, (3) references to the COPYING file, (4) an identification of SourceForge or JMRI as the original source of the definition files, and (5) a description of how the files or computer code had been changed from the original source code. The Decoder Commander software also changed various computer file names of DecoderPro files without providing a reference to the original JMRI files or information on where to get the Standard Version.[1]

[1] Katzer/Kamind represents that all potentially infringing activities using any of the disputed material have been voluntarily ceased. The district court held that it could not find as a matter of law that Katzer/Kamind's voluntary termination of allegedly wrongful activity renders the motion for preliminary injunction moot because it could not find as a matter of law that it is absolutely clear that the alleged behavior could not recur. Jacobsen, 2007 WL 2358628 at *5. We agree that this matter is not moot. See also Adarand Constructors, Inc. v. Slater, 528 U.S. 216, 222 (2000) ("Voluntary cessation of challenged conduct moots a case . . . only if it is absolutely clear that the allegedly wrongful behavior could not reasonably be expected to recur." (emphasis in original)).

Jacobsen moved for a preliminary injunction, arguing that the violation of the terms of the Artistic License constituted copyright infringement and that, under Ninth Circuit law, irreparable harm could be presumed in a copyright infringement case. The District Court reviewed the Artistic License and determined that "Defendants' alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license, but does not create liability for copyright infringement where it would not otherwise exist." Id. at *7. The District Court found that Jacobsen had a cause of action only for breach of contract, rather than an action for copyright infringement based on a breach of the conditions of the Artistic License. Because a breach of contract creates no presumption of irreparable harm, the District Court denied the motion for a preliminary injunction.

Jacobsen appeals the finding that he does not have a cause of action for copyright infringement. Although an appeal concerning copyright law and not patent law is rare in our Circuit, here we indeed possess appellate jurisdiction. In the district court, Jacobsen's operative complaint against Katzer/Kamind included not only his claim for copyright infringement, but also claims seeking a declaratory judgment that a patent issued to Katzer is not infringed by Jacobsen and is invalid. Therefore the complaint arose in part under the patent laws. See 28 U.S.C. § 2201(a); Golan v. Pingel Enter., 310 F.3d 1360, 1367 (Fed. Cir. 2002) (explaining that "[i]n the context of a complaint seeking a declaration of noninfringement, the action threatened by the declaratory defendant . . . would be an action for patent infringement," and "[s]uch an action clearly arises under the patent laws"). Thus the district court's jurisdiction was based, at least in part, on 28 U.S.C. § 1338(a) as it relates to the patent laws, and we have appellate jurisdiction under 28 U.S.C. § 1292(c)(1). See 28 U.S.C. § 1338(a) ("The district courts shall have original jurisdiction of any civil

action arising under any Act of Congress relating to patents, plant variety protection, copyrights and trademarks."); id. at § 1295(a)(1) (The Federal Circuit shall have exclusive jurisdiction "of an appeal from a final decision of a district court of the United States" if (1) "the jurisdiction of that court was based, in whole or in part, on section 1338 of this title" and (2) the case is not "a case involving a claim arising under any Act of Congress relating to copyrights, exclusive rights in mask works, or trademarks and no other claims under section 1338(a)."); id. at § 1292(c)(1) (Federal Circuit shall have jurisdiction over appeals from interlocutory orders of the district courts refusing injunctions "in any case over which the court would have jurisdiction of an appeal under section 1295").

II.

This Court looks to the interpretive law of the regional circuit for issues not exclusively assigned to the Federal Circuit. Hutchins v. Zoll Med. Corp., 492 F.3d 1377, 1383 (Fed. Cir. 2007). Under Ninth Circuit law, an order granting or denying a preliminary injunction will be reversed only if the district court relied on an erroneous legal premise or abused its discretion. Wright v. Rushen, 642 F.2d 1129, 1132 (9th Cir. 1981). A district court's order denying a preliminary injunction is reversible for factual error only when the district court rests its conclusions on clearly erroneous findings of fact. Sports Form, Inc. v. United Press Int'l, Inc., 686 F.2d 750, 753 (9th Cir. 1982).

In determining whether to issue a preliminary injunction, the Ninth Circuit requires demonstration of (1) a combination of probability of success on the merits and the possibility of irreparable harm; or (2) serious questions going to the merits where the balance of hardships tips sharply in the moving party's favor. Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 713-14 (9th Cir. 2007); Dep't of Parks & Recreation v.

Bazaar Del Mundo, Inc., 448 F.3d 1118, 1123 (9th Cir. 2006). In cases involving copyright claims, where a copyright holder has shown likelihood of success on the merits of a copyright infringement claim, the Ninth Circuit has held that irreparable harm is presumed. LGS Architects, Inc. v. Concordia Homes of Nev., 434 F.3d 1150, 1155-56 (9th Cir. 2006). But see MGM Studios, Inc. v. Grokster, Ltd., 518 F. Supp. 2d 1197, 1212 (C.D. Cal. 2007) (noting that "the longstanding rule that irreparable harm can be a presumed after a showing of likelihood of success for purposes of a copyright preliminary injunction motion may itself have to be reevaluated in light of eBay [Inc. v. MercExchange, L.L.C., 547 U.S. 388 (2006)]"). Thus, for a preliminary injunction to issue, Jacobsen must either show (1) a likelihood of success on the merits of his copyright infringement claim from which irreparable harm is presumed; or (2) a fair chance of success on the merits and a clear disparity in the relative hardships that tips sharply in his favor.

A.

Public licenses, often referred to as "open source" licenses, are used by artists, authors, educators, software developers, and scientists who wish to create collaborative projects and to dedicate certain works to the public. Several types of public licenses have been designed to provide creators of copyrighted materials a means to protect and control their copyrights. Creative Commons, one of the amici curiae, provides free copyright licenses to allow parties to dedicate their works to the public or to license certain uses of their works while keeping some rights reserved.

Open source licensing has become a widely used method of creative collaboration that serves to advance the arts and sciences in a manner and at a pace that few could have imagined just a few decades ago. For example, the Massachusetts Institute of

Technology ("MIT") uses a Creative Commons public license for an OpenCourseWare project that licenses all 1800 MIT courses. Other public licenses support the GNU/Linux operating system, the Perl programming language, the Apache web server programs, the Firefox web browser, and a collaborative web-based encyclopedia called Wikipedia. Creative Commons notes that, by some estimates, there are close to 100,000,000 works licensed under various Creative Commons licenses. The Wikimedia Foundation, another of the amici curiae, estimates that the Wikipedia website has more than 75,000 active contributors working on some 9,000,000 articles in more than 250 languages.

Open Source software projects invite computer programmers from around the world to view software code and make changes and improvements to it. Through such collaboration, software programs can often be written and debugged faster and at lower cost than if the copyright holder were required to do all of the work independently. In exchange and in consideration for this collaborative work, the copyright holder permits users to copy, modify and distribute the software code subject to conditions that serve to protect downstream users and to keep the code accessible.[2] By requiring that users copy and restate the license and attribution information, a copyright holder can ensure that recipients of the redistributed computer code know the identity of the owner as well as the scope of the license granted by the original owner. The Artistic License in this case also requires that changes to the computer code be tracked so that downstream users know what part of the computer code is the original code created by the copyright holder and what part has been newly added or altered by another collaborator.

[2] For example, the GNU General Public License, which is used for the Linux operating system, prohibits downstream users from charging for a license to the software. See Wallace v. IBM Corp., 467 F.3d 1104, 1105-06 (7th Cir. 2006).

Traditionally, copyright owners sold their copyrighted material in exchange for money. The lack of money changing hands in open source licensing should not be presumed to mean that there is no economic consideration, however. There are substantial benefits, including economic benefits, to the creation and distribution of copyrighted works under public licenses that range far beyond traditional license royalties. For example, program creators may generate market share for their programs by providing certain components free of charge. Similarly, a programmer or company may increase its national or international reputation by incubating open source projects. Improvement to a product can come rapidly and free of charge from an expert not even known to the copyright holder. The Eleventh Circuit has recognized the economic motives inherent in public licenses, even where profit is not immediate. See Planetary Motion, Inc. v. Techsplosion, Inc., 261 F.3d 1188, 1200 (11th Cir. 2001) (Program creator "derived value from the distribution [under a public license] because he was able to improve his Software based on suggestions sent by end-users. . . . It is logical that as the Software improved, more end-users used his Software, thereby increasing [the programmer's] recognition in his profession and the likelihood that the Software would be improved even further.").

B.

The parties do not dispute that Jacobsen is the holder of a copyright for certain materials distributed through his website.[3] Katzer/Kamind also admits that portions of the DecoderPro software were copied, modified, and distributed as part of the Decoder Commander software. Accordingly, Jacobsen has made out a prima facie case of copyright infringement. Katzer/Kamind argues that they cannot be liable for copyright

[3] Jacobsen's copyright registration creates the presumption of a valid copyright.

infringement because they had a license to use the material. Thus, the Court must evaluate whether the use by Katzer/Kamind was outside the scope of the license. See LGS Architects, 434 F.3d at 1156. The copyrighted materials in this case are downloadable by any user and are labeled to include a copyright notification and a COPYING file that includes the text of the Artistic License. The Artistic License grants users the right to copy, modify, and distribute the software:

> provided that [the user] insert a prominent notice in each changed file stating how and when [the user] changed that file, and provided that [the user] do at least ONE of the following:
> a) place [the user's] modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include [the user's] modifications in the Standard Version of the Package.
> b) use the modified Package only within [the user's] corporation or organization.
> c) rename any non-standard executables so the names do not conflict with the standard executables, which must also be provided, and provide a separate manual page for each nonstandard executable that clearly documents how it differs from the Standard Version, or
> d) make other distribution arrangements with the Copyright Holder.

The heart of the argument on appeal concerns whether the terms of the Artistic License are conditions of, or merely covenants to, the copyright license. Generally, a "copyright owner who grants a nonexclusive license to use his copyrighted material waives his right to sue the licensee for copyright infringement" and can sue only for breach of contract. Sun Microsystems, Inc., v. Microsoft Corp., 188 F.3d 1115, 1121 (9th Cir. 1999); Graham v. James, 144 F.3d 229, 236 (2d Cir. 1998). If, however, a license is limited in scope and the licensee acts outside the scope, the licensor can bring an action for

---

See, e.g., Triad Sys. Corp. V. Se. Exp. Co., 64 F.3d 1330, 1335 (9th Cir. 1995).

copyright infringement. See S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081, 1087 (9th Cir.1989); Nimmer on Copyright, § 1015[A] (1999).

Thus, if the terms of the Artistic License allegedly violated are both covenants and conditions, they may serve to limit the scope of the license and are governed by copyright law. If they are merely covenants, by contrast, they are governed by contract law. See Graham, 144 F.3d at 236-37 (whether breach of license is actionable as copyright infringement or breach of contract turns on whether provision breached is condition of the license, or mere covenant); Sun Microsystems, 188 F.3d at 1121 (following Graham; independent covenant does not limit scope of copyright license). The District Court did not expressly state whether the limitations in the Artistic License are independent covenants or, rather, conditions to the scope; its analysis, however, clearly treated the license limitations as contractual covenants rather than conditions of the copyright license.[4]

Jacobsen argues that the terms of the Artistic License define the scope of the license and that any use outside of these restrictions is copyright infringement. Katzer/Kamind argues that these terms do not limit the scope of the license and are merely covenants providing contractual terms for the use of the materials, and that his violation of them is neither compensable in damages nor subject to injunctive relief. Katzer/Kamind's argument is premised upon the assumption that Jacobsen's copyright gave him no economic rights because he made his computer code available to the public at no charge. From this assumption, Katzer/Kamind argues that copyright law does not recognize a

[4] The District Court held that "Defendants' alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license . . . [and] the Court finds that Plaintiff's claim properly sounds in contract." Jacobsen, 2007 WL 2358628 at *7. Thus, despite the use of the word "conditions," the District Court treated the terms of the Artistic License as contractual covenants which did not limit the scope of the license.

cause of action for non-economic rights, relying on Gilliam v. ABC, 538 F.2d 14, 20-21 (2d Cir. 1976) ("American copyright law, as presently written, does not recognize moral rights or provide a cause of action for their violation, since the law seeks to vindicate the economic, rather than the personal rights of authors."). The District Court based its opinion on the breadth of the Artistic License terms, to which we now turn.

III.

The Artistic License states on its face that the document creates conditions: "The intent of this document is to state the conditions under which a Package may be copied." (Emphasis added.) The Artistic License also uses the traditional language of conditions by noting that the rights to copy, modify, and distribute are granted "provided that" the conditions are met. Under California contract law, "provided that" typically denotes a condition. See, e.g., Diepenbrock v. Luiz, 159 Cal. 716 (1911) (interpreting a real property lease reciting that when the property was sold, "this lease shall cease and be at an end, provided that the party of the first part shall then pay [certain compensation] to the party of the second part"; considering the appellant's "interesting and ingenious" argument for interpreting this language as creating a mere covenant rather than a condition; and holding that this argument "cannot change the fact that, attributing the usual and ordinary signification to the language of the parties, a condition is found in the provision in question") (emphases added).

The conditions set forth in the Artistic License are vital to enable the copyright holder to retain the ability to benefit from the work of downstream users. By requiring that users who modify or distribute the copyrighted material retain the reference to the original source files, downstream users are directed to Jacobsen's website. Thus, downstream users

know about the collaborative effort to improve and expand the SourceForge project once they learn of the "upstream" project from a "downstream" distribution, and they may join in that effort.

The District Court interpreted the Artistic License to permit a user to "modify the material in any way" and did not find that any of the "provided that" limitations in the Artistic License served to limit this grant. The District Court's interpretation of the conditions of the Artistic License does not credit the explicit restrictions in the license that govern a downloader's right to modify and distribute the copyrighted work. The copyright holder here expressly stated the terms upon which the right to modify and distribute the material depended and invited direct contact if a downloader wished to negotiate other terms. These restrictions were both clear and necessary to accomplish the objectives of the open source licensing collaboration, including economic benefit. Moreover, the District Court did not address the other restrictions of the license, such as the requirement that all modification from the original be clearly shown with a new name and a separate page for any such modification that shows how it differs from the original.

Copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material. As the Second Circuit explained in Gilliam v. ABC, 538 F.2d 14, 21 (2d Cir. 1976), the "unauthorized editing of the underlying work, if proven, would constitute an infringement of the copyright in that work similar to any other use of a work that exceeded the license granted by the proprietor of the copyright." Copyright licenses are designed to support the right to exclude; money damages alone do not support or enforce that right. The choice to exact consideration in the form of compliance with the open source requirements of disclosure and explanation of changes,

rather than as a dollar-denominated fee, is entitled to no less legal recognition. Indeed, because a calculation of damages is inherently speculative, these types of license restrictions might well be rendered meaningless absent the ability to enforce through injunctive relief.

In this case, a user who downloads the JMRI copyrighted materials is authorized to make modifications and to distribute the materials "provided that" the user follows the restrictive terms of the Artistic License. A copyright holder can grant the right to make certain modifications, yet retain his right to prevent other modifications. Indeed, such a goal is exactly the purpose of adding conditions to a license grant.[5] The Artistic License, like many other common copyright licenses, requires that any copies that are distributed contain the copyright notices and the COPYING file. See, e.g., 3-10 Nimmer on Copyright § 10.15 ("An express (or possibly an implied) condition that a licensee must affix a proper copyright notice to all copies of the work that he causes to be published will render a publication devoid of such notice without authority from the licensor and therefore, an infringing act.").

It is outside the scope of the Artistic License to modify and distribute the copyrighted materials without copyright notices and a tracking of modifications from the original computer files. If a downloader does not assent to these conditions stated in the COPYING

[5] Open source licensing restrictions are easily distinguished from mere "author attribution" cases. Copyright law does not automatically protect the rights of authors to credit for copyrighted materials. See Gilliam, 538 F.2d at 20-21 ("American copyright law, as presently written, does not recognize moral rights or provide a cause of action for their violation, since the law seeks to vindicate the economic, rather than the personal rights of authors."); Graham, 144 F.3d at 236. Whether such rights are protected by a specific license grant depends on the language of the license. See County of Ventura v. Blackburn, 362 F.2d 515, 520 (9th Cir. 1966) (copyright infringement found where the county removed copyright notices from maps licensed to it where the license granted the county "the right to

file, he is instructed to "make other arrangements with the Copyright Holder." Katzer/Kamind did not make any such "other arrangements." The clear language of the Artistic License creates conditions to protect the economic rights at issue in the granting of a public license. These conditions govern the rights to modify and distribute the computer programs and files included in the downloadable software package. The attribution and modification transparency requirements directly serve to drive traffic to the open source incubation page and to inform downstream users of the project, which is a significant economic goal of the copyright holder that the law will enforce. Through this controlled spread of information, the copyright holder gains creative collaborators to the open source project; by requiring that changes made by downstream users be visible to the copyright holder and others, the copyright holder learns about the uses for his software and gains others' knowledge that can be used to advance future software releases.

IV.

---

obtain duplicate tracings" from photographic negatives that contained copyright notices).

For the aforementioned reasons, we vacate and remand. While Katzer/Kamind appears to have conceded that they did not comply with the aforedescribed conditions of the Artistic License, the District Court did not make factual findings on the likelihood of success on the merits in proving that Katzer/Kamind violated the conditions of the Artistic License. Having determined that the terms of the Artistic License are enforceable copyright conditions, we remand to enable the District Court to determine whether Jacobsen has demonstrated (1) a likelihood of success on the merits and either a presumption of irreparable harm or a demonstration of irreparable harm; or (2) a fair chance of success on the merits and a clear disparity in the relative hardships and tipping in his favor.[6]

The judgment of the District Court is vacated and the case is remanded for further proceedings consistent with this opinion.

VACATED and REMANDED

[6] At oral argument, the parties admitted that there might be no way to calculate any monetary damages under a contract theory.

NOT FOR PUBLICATION

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

ROBERT JACOBSEN,

Plaintiff,

v.

MATTHEW KATZER and KAMIND ASSOCIATES, INC.,

Defendants.

_____/

No. C 06-01905 JSW

ORDER GRANTING MOTION TO DISMISS FOR MOOTNESS; DENYING IN PART AND GRANTING IN PART MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM; DENYING MOTION TO STRIKE; AND DENYING MOTION FOR PRELIMINARY INJUNCTION

Now before the Court are the motions filed by Matthew Katzer and Kamind Associates, Inc. ("KAM") to dismiss counts one, two and three for mootness and the motion to dismiss counts five and six for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6) and to strike portions of the second amended complaint pursuant to Federal Rule of Civil Procedure 12(f). Also before the Court is Jacobsen's second motion for preliminary injunction on his copyright claim. Having carefully reviewed the parties' papers, considered their arguments and the relevant legal authority, the Court hereby GRANTS Defendants' motion to dismiss for mootness; GRANTS IN PART AND DENIES IN PART Defendants' motion to dismiss for failure to state a claim; DENIES the motion to strike; and DENIES Jacobsen's motion for preliminary injunction.

BACKGROUND

Matthew Katzer is the chief executive officer and chairman of the board of directors of KAM, a software company based in Portland, Oregon that develops software for model railroad

enthusiasts. The Java Model Railroad Interface ("JMRI") Project is an on-line, open source community that also develops model train software. Plaintiff, Robert Jacobsen, works for the Lawrence Berkeley National Laboratory and is a professor of physics at the university, as well as a model train hobbyist and a leading member of the JMRI Project.

According to the second amended complaint, Jacobsen contends that Defendants fraudulently secured patents for their software and, despite knowing the patents were invalid and unenforceable, sought to enforce the patents and collect patent royalties, and threatened litigation. Jacobsen makes claims for declaratory judgment of the unenforceability and invalidity of KAM's patent, non-infringement of Jacobsen's work, violation of copyright laws, violation of the Digital Millenium Copyright Act ("DMCA"), breach of contract under California law, and cybersquatting in violation of 15 U.S.C. § 1125(d).

Now before the Court is Defendants' motion to dismiss the first, second and third claims for relief for declaratory judgment on unenforceability and invalidity of KAM's patent and non-infringement of Jacobsen's work on the basis that withdrawal of the patent in dispute renders the claims moot and the Court without jurisdiction to hear those claims. Defendants further move to dismiss claims five and six for violations of the DMCA and for breach of contract for failure to state a claim upon which relief can be granted. In this same motion, Defendants move to strike Jacobsen's prayer for relief for attorneys' fees under 17 U.S.C. §§ 504 and 505 pursuant to Federal Rule of Civil Procedure 12(f). Lastly, Jacobseon moves for preliminary injunction, seeking to have the Court enjoin Defendants from willfully infringing his copyrighted material.

The Court shall refer to additional facts as necessary in the remainder of this Order.

ANALYSIS

A. Matthew Katzer and Kamind Associates, Inc.'s Motion to Dismiss for Mootness.

1. Legal Standard on Motion to Dismiss Pursuant to Federal Rule of Civil Procedure 12(b)(1).

When a defendant moves to dismiss a complaint or claim for lack of subject matter jurisdiction, the plaintiff bears the burden of proving that the court has jurisdiction to decide the claim. *Thornhill Publ'n Co. v. Gen. Tel. & Elecs. Corp.*, 594 F.2d 730, 733 (9th Cir. 1979).

Federal courts can only adjudicate cases which the Constitution or Congress authorize them to adjudicate: those cases which involve diversity of citizenship, or those cases which involve a federal question, or those cases which involve the United States as a party. *See e.g., Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994).

A motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) may be "facial or factual." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). Where an attack on jurisdiction is a "facial" attack on the allegations of the complaint, the factual allegations of the complaint are taken as true and the non-moving party is entitled to have those facts construed in the light most favorable to him or her. *Fed'n of African Am. Contractors v. City of Oakland*, 96 F.3d 1204, 1207 (9th Cir. 1996). If the jurisdictional attack is "factual," a defendant may rely on affidavits or other evidence properly before the Court, and the non-moving party is not entitled to any presumptions of truthfulness with respect to the allegations in the complaint. Rather, he or she must come forward with evidence establishing jurisdiction. *Thornhill*, 594 F.2d at 733.

Lack of subject matter jurisdiction may be raised at any stage in the litigation. *Morongo Band of Mission Indians v. Cal. State Board of Equalization*, 858 F.2d 1376, 1380 (9th Cir. 1988). In assessing the scope of its jurisdiction, the Court may consider evidence extrinsic to the allegations in the complaint. *Augustine v. United States*, 704 F.2d 1074, 1077 (9th Cir. 1983).

2. Patent Declaratory Claims Are Mooted by Disclaimer.

Counts one, two and three of the second amended complaint must be dismissed as moot because of Defendants' disclaimer of the patent sued upon. The Defendants filed a Disclaimer in Patent under 37 C.F.R. § 1.321(a) with the Patent and Trademark Office on February 1, 2008, disclaiming all claims in the '329 patent. (*See* Declaration of Matthew Katzer, ¶ 3, Ex. A.) There is no dispute that the patent at issue in this case has been disclaimed and there is therefore no further substantial controversy between the parties of "sufficient immediacy and reality to warrant the issuance of a declaratory judgment." *See MedImmune, Inc. v. Genentech, Inc.*, 127

S. Ct. 764, 771 (2007). The Supreme Court set forth the correct standard for jurisdiction over a declaratory relief action:

> [T]hat the dispute be definite and concrete, touching the legal relations having adverse legal interests and that it be real and substantial and admit of specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts.

Id. at 774 n.11 (citing *Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 240 (1937)).

"A patentee defending an action for a declaratory judgment of invalidity can divest the trial court of jurisdiction over the case by filing a covenant not to assert the patent at issue against the putative infringer with respect to any of its past, present of future acts...." *Super Sack Mfg. Corp. v. Chase Packaging Corp.*, 57 F.3d 1054, 1058 (Fed. Cir. 1995). Despite the more recent ruling in *MedImmune*, this fundamental concept remains the same. *See Benitec Australia, Ltd. v. Nucleonics, Inc.*, 495 F.3d 1340, 1343-44 (9th Cir. 2007); *Crossbow Tech., Inc. v. YH Tech.*, 531 F. Supp. 2d 1117, 1124 (N.D. Cal. 2007). A declaratory judgment action relating to the enforceability of a disclaimed patent is moot.

In opposition to the motion to dismiss for mootness, Jacobsen argues that he has suffered damages in the amount of the award of attorneys' fees granted in connection with Defendants' California anti-SLAPP ("Strategic Lawsuit Against Public Participation") motion.[1] The anti-SLAPP motion damages were awarded in connection with the filing of a claim for libel because the claim was based on the filing of a FOIA request to the Department of Energy, which is a protected communication under California's anti-SLAPP statute as it was made in anticipation of bringing legal action against Jacobsen. *See* Cal. Code Civil Proc. § 425.16(b)(1). The damages in the form of attorneys' fees paid to compensate for the filing of a libel claim simply does not constitute a recognizable injury for the purposes of continuing to litigate a patent claim for a patent that has been disclaimed. The damages incurred in the litigation of the libel claim do not give Jacobsen standing to create a substantial controversy

[1] The opposition to the motion to dismiss for mootness reads like a motion for reconsideration of the Court's decision on the anti-SLAPP motion. To the degree it can be construed as a motion to reconsider, it is DENIED.

between the parties of "sufficient immediacy and reality to warrant the issuance of a declaratory judgment." *See MedImmune*, 127 S. Ct. at 771.

Jacobsen also alludes to the possibility that Defendants own other patents which may be relevant to this litigation. However, there is nothing in the record to support the position that there is a substantial controversy between the parties to merit retaining jurisdiction over the declaratory claim. Defendants maintain they have no intent to sue Jacobsen over alternate patents and any determination regarding patents not yet in suit would render the Court's opinion merely, and impermissibly, advisory. *See Micron Technology, Inc. v. Mosaid Technologies, Inc.*, 518 F.3d 897, 901-02 (Fed. Cir. 2008).

Lastly, Jacobsen also argues that he has standing to litigate a disclaimed patent because, under 35 U.S.C. § 285, he has incurred attorneys' fees in the litigation over the past two years and has standing to allege injury as a result. However, section 285 provides only that the court may, in exceptional cases, award reasonable attorney fees to the prevailing party. To be eligible for an award of attorneys' fees under section 285, Jacobsen must first demonstrate that he is the prevailing party on the patent claims. Here, Defendants voluntarily disclaimed the patent at issue. Although Jacobsen argues that the disclaimer was the result of the settlement conference magistrate judge's order requiring the parties to proffer their positions on the patent, as well as the other claims, Defendants were never ordered to disclaim the patent and did so voluntarily. "A defendant's voluntary change in conduct, although perhaps accomplishing what the plaintiff sought to achieve by the lawsuit, lacks the necessary judicial *imprimatur* on the change. Our precedents thus counsel against holding that the term 'prevailing party' authorizes an award of attorney's fees *without* a corresponding alteration in the legal relationship of the parties." *Buckhannon Bd. and Care Home, Inc. v. West Virginia Dept. of Health and Human Resources*, 532 U.S. 598, 605 (2001) (emphasis in original).

Because, as the patent at issue was voluntarily disclaimed, the Court cannot find that Jacobsen is the prevailing party in this matter. Therefore, attorneys' fees under section 285 could not become available to Jacobsen and does not, in any case, form an independent basis for jurisdiction over the now-disclaimed patent. Accordingly, the Court finds no basis for retaining

jurisdiction over the patent dispute in this case, and therefore dismisses counts one, two and three without leave to amend.[2]

B. Matthew Katzer and Kamind Associates, Inc.'s Motion to Dismiss for Failure to State a Claim Upon Which Relief Can Be Granted.

1. Legal Standard on Motion to Dismiss Pursuant to Federal Rule of Civil Procedure 12(b)(6).

A motion to dismiss is proper under Federal Rule of Civil Procedure 12(b)(6) where the pleadings fail to state a claim upon which relief can be granted. The complaint is construed in the light most favorable to the non-moving party and all material allegations in the complaint are taken to be true. *Sanders v. Kennedy,* 794 F.2d 478, 481 (9th Cir. 1986). The court, however, is not required to accept legal conclusions cast in the form of factual allegations, if those conclusions cannot reasonably be drawn from the facts alleged. *Clegg v. Cult Awareness Network*, 18 F.3d 752, 754-55 (9th Cir. 1994) (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)). Conclusory allegations without more are insufficient to defeat a motion to dismiss for failure to state a claim upon which relief may be granted. *McGlinchy v. Shell Chemical Co.*, 845 F.2d 802, 810 (9th Cir. 1988). Even under the liberal pleading standard of Federal Rule of Civil Procedure 8(a)(2), a plaintiff must do more than recite the elements of the claim and must "provide the grounds of [its] entitlement to relief." *Bell Atlantic v. Twombly*, 127 S. Ct. 1955, 1959 (2007) (citations omitted). In addition, the pleading must not merely allege conduct that is conceivable, but it must also be plausible. *Id.* at 1974.

2. Claim for Breach of Contract.

In order to state a claim for breach of contract, Jacobsen must allege (1) the existence of a contract; (2) plaintiff's performance or excuse for non-performance; (3) defendants' breach and damage to plaintiff proximately caused from defendants' breach. *See Acoustics, Inc. v. Trepte Construction Co.*, 14 Cal. App. 3d 887, 913 (1971) (citing 2 Witkin, Cal. Proc., Pleading, § 251). Jacobsen has failed to allege a specific harm that was proximately caused by

[2] Although addressed by the Court at oral argument, for the sake of clarity, Jacobsen's motion for leave to file a sur-reply to Defendants' motion to dismiss for mootness is DENIED. The sur-reply and all attached declarations and exhibits are HEREBY STRICKEN from the record. In addition, Jacobsen's motion to strike portions of the declarations of Matthew Katzer and Kevin Russell is DENIED.

the alleged breach of the terms of the Artistic License. The Second Amended Complaint merely states that "[b]y reason of the breach, Plaintiff has been harmed" and seeks "rescission, and disgorgement of the value he conferred on Defendants, plus interest and costs." (Second Amended Complaint, ¶¶ 491, 492.) The complaint does not state the proximate cause of the alleged damage, nor does it state what the actual damage was incurred by Jacobsen. The Federal Circuit, in its decision on the appeal of this Court's order denying Jacobsen's motion for a preliminary injunction, opines that damage to the "creation and distribution of copyrighted works under public licenses" could include injury to reputation and the programmers' recognition in his profession as well as impact on the likelihood that the product will be further improved. *Jacobsen v. Katzer*, 535 F.3d 1373, 1379 (Fed. Cir. 2008) (finding that the lack of money changing hands in open source licensing should not be presumed to mean that there is no economic consideration). The appellate decision enumerates these potential damages which could have been caused by Defendants' activity in interfering with open source licensing. However, as the claim for breach of contract is currently drafted, there is no indication what, if any, damages Jacobsen claims to have incurred that were the proximate cause of a breach of the Artistic License. For this reason, the allegations for breach of contract fail to state a claim upon which relief can be granted and the claim is dismissed with leave to amend.

Although the claim for breach of contract fails to state a claim upon which relief can be granted for failure to state damages proximately caused by the alleged breach, the Court also finds that the state law claim, as drafted, is also preempted by federal copyright law.

Section 301 of the Federal Copyright Act provides in pertinent part:

> all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright ... are governed exclusively by this title. Thereafter, no person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State.

17 U.S.C. § 301. The federal copyright preemption of overlapping state law claims is "explicit and broad." *G.S. Rasmussen & Assoc. V. Kalitta Flying Serv.*, 958 F.2d 896, 904 (9th Cir. 1992). Section 301 of the Copyright Act establishes a two-part test for preemption. First, the claims must come within the subject matter of copyright, and (2) the rights granted under state law must be equivalent to any of the exclusive rights within the general scope of copyright as

set forth in the Act. *Del Madera Props. v. Rhodes & Gardner*, 820 F.2d 973, 976 (9th Cir. 1987). The claim for breach of contract addresses the subject matter that is within the subject matter of the Copyright Act as the claim deals exclusively with the misappropriation of the JMRI Project decoder definition files. (*See* Second Amended Complaint, ¶¶ 486-492 (alleging that Defendants accepted Plaintiff's offer to permit the use of the Decoder Definition files, subject to the Artistic License, but failed to perform the agreement to honor any of the terms or conditions of the Artistic License).)

To satisfy the "equivalent rights" part of the preemption test, Jacobsen's contract claim. which is predicated upon the alleged use of the copyrighted work without abiding by the terms of the Artistic License, must be equivalent to rights within the general scope of copyright. *See Del Madera*, 820 F.2d at 977. In other words, to survive preemption, the state cause of action must protect rights which are qualitatively different from the copyright rights. *Id.* (citing *Harper & Row, Publishers, Inc. v. Nation Enterprises*, 501 F. Supp. 848, 852 (S.D.N.Y. 1980)). The state claim must have an "extra element" which changes the nature of the action. *Id.* (citing *Mayer v. Josiah Wedgwood & Sons, Ltd.*, 601 F. Supp. 1523, 1535 (S.D.N.Y. 1985)).

The breach of contract claim does not add an "extra element" which changes the nature of the action or the rights secured under federal copyright protection. The breach of contract claim alleges violations of the exact same exclusive federal rights protected by Section 106 of the Copyright Act, the exclusive right to reproduce, distribute and make derivative copies.

Accordingly, the breach of contract claim is preempted by federal copyright law, and is thereby dismissed on this alternate basis with leave to amend. Should Jacobsen wish to amend his complaint, he will not only have to make an allegation of damages proximately caused by the alleged breach of the Artistic License, but will, in addition, have to state a claim that is not preempted by federal copyright law by demonstrating that there are rights or remedies available under the contract claims that are not otherwise available under the copyright claim.

3. Claim Under DMCA.

Jacobsen alleges that the information contained in the JMRI Project Decoder Definition Files constituted "copyright management information" within the meaning of the Digital

Millennium Copyright Act and that by removing the information and making copies of the files, Defendants violated 17 U.S.C. § 1201(b), which protects the integrity of copyright management information.

Under the statute, the term copyright management information ("CMI") means "any of the following information conveyed in connection with copies ... of a work ..., including digital form," including "the name of, and other identifying information about the author of the work, ... the copyright owner of the work, ... [and other] information identifying the work." 17 U.S.C. § 1202(c). The information Jacobsen contends consists of copyright management information in his complaint is the "author's name, a title, a reference to the license and where to find the license, a copyright notice, and the copyright owner." (Second Amended Complaint, ¶ 479.) Jacobsen also alleges that he used a software script to automate adding copyright notices and information regarding the license and uploaded the files on the internet through SourceForge.net, an open source incubator website. (*Id.*, ¶¶ 267, 480.) Jacobsen contends that Defendants downloaded the files and removed the names of the authors and copyright holder, title, reference to license, where to find the license and the copyright notices, and instead, renamed the files and referred to their own copyright notice and named themselves as author and copyright owner. (*Id.*, ¶¶ 271-76; 289-291.)

Although the law on the definition and application in practice of the term CMI is scant, the Court finds that it would be premature to dismiss the claim on the facts as alleged. *See Electrical Construction & Maintenance Co. v. Maeda Pacific Corp.*, 764 F.2d 619, 623 (9th Cir. 1985) ("The court should be especially reluctant to dismiss on the basis of the pleadings when the asserted theory of liability is novel ..., since it is important that new legal theories be explored and assayed in the light of actual facts."). In *IQ Group v. Wiesner Publishing, Inc.*, the court, at the summary judgment stage, determined after a lengthy review of the legislative history of the DMCA that the statute should be construed to protect CMI performed by the technological measures of automated systems. 400 F. Supp. 2d 587, 597 (D. N.J. 2006). In *McClatchey v. The Associated Press*, because the plaintiff had used a computer software program to print her title, name and copyright notice on copies of her photograph, the district

court determined that this technological process came within the term CMI as defined in section 1202(c). 2007 WL 776103, *5 (W.D. Pa. March 9, 2007).

Based on the allegations in the complaint, the Court finds that there has been some technological process engaged to protect the author's name, a title, a reference to the license and where to find the license, a copyright notice, and the copyright owner of Jacobsen's work. Therefore, without further discovery, the Court finds that it would be inappropriate to dismiss the cause of action for violation of the DMCA.

4. Motion to Strike Attorneys' Fees Prayer for Relief.

Federal Rule of Civil Procedure 12(f) provides that a court may "order stricken from any pleading any insufficient defense or any redundant, immaterial, impertinent, or scandalous matter." Immaterial matter "is that which has no essential or important relationship to the claim for relief or the defenses being pleaded." *California Dept. of Toxic Substance Control v. ALCO Pacific, Inc.*, 217 F. Supp. 2d 1028, 1032 (C.D. Cal. 2002) (internal citations and quotations omitted). Impertinent material "consists of statements that do not pertain, or are not necessary to the issues in question." *Id*. Motions to strike are regarded with disfavor because they are often used as delaying tactics and because of the limited importance of pleadings in federal practice. *Colaprico v. Sun Microsystems Inc.*, 758 F. Supp 1335, 1339 (N.D. Cal. 1991). The possibility that issues will be unnecessarily complicated or that superfluous pleadings will cause the trier of fact to draw unwarranted inferences at trial is the type of prejudice that is sufficient to support the granting of a motion to strike. *Cal. Dept. of Toxic Substances Control*, 217 F. Supp. at 1028. Under Rule 12(f), courts have authority to strike a prayer for relief seeking damages that are not recoverable as a matter of law. *Wells v. Board of Trustees of the Cal. State Univ.*, 393 F. Supp. 2d 990, 994-95 (N.D. Cal. 2005); *Arcilla v. Adidas Promotional Retail Operations, Inc.*, 488 F. Supp. 2d 965, 968 (C.D. Cal. 2007) (citing *Tapley v. Lockwood Green Engineers, Inc.*, 502 F.2d 559, 560 (8th Cir. 1974)).

Defendants contend that Jacobsen is not entitled to seek damages under 17 U.S.C. §§ 504 and 505 because Jacobsen registered the copyright on June 13, 2006 after the alleged infringement occurred. However, because there are allegations that the alleged infringement

occurred earlier and because the allegations of infringement may not be complete, the Court finds it would be premature to dismiss the claims for damages at this time. (*See, e.g.*, Second Amended Complaint, ¶ 266.) Although the allegations in the complaint as to the timing of the alleged instances of infringement constitute a compelling statement of the dates of alleged infringement, the Court finds that, by virtue of discovery, Jacobsen may find additional instances of infringement and therefore, Defendants' motion to strike is premature.

C. Jacobsen's Motion for Preliminary Injunction on Copyright Claim.

1. Legal Standard.

Plaintiff moves for preliminary injunction, seeking a court order enjoining Defendants from willfully infringing Plaintiff's copyrighted material. A plaintiff is entitled to a preliminary injunction when it can demonstrate either: (1) a combination of probable success on the merits and the possibility of irreparable injury, or (2) the existence of serious questions going to the merits, where the balance of hardships tips sharply in plaintiff's favor. *GoTo.com, Inc. v. Walt Disney Co.*, 202 F.3d 1199, 1204-05 (9th Cir. 2000). To establish copyright infringement, a plaintiff must show (1) ownership of the copyrights, and (2) copying of the protected expression by Defendants. *Sun Microsystems, Inc. v. Microsoft Corp.*, 188 F.3d 1115, 1109 (9th Cir. 1999).

Initially, when this matter was before the Court on a motion for preliminary injunction, federal copyright law provided that a plaintiff who demonstrates a likelihood of success on the merits of a copyright claim was automatically entitled to a presumption of irreparable harm. *Id.* at 1119 (citing *Cadence Design Systems v. Avant! Corp.*, 125 F.3d 824, 826-27 (9th Cir. 1997)). "That presumption means that the balance of hardships issue cannot be accorded significant – if any – weight in determining whether a court should enter a preliminary injunction to prevent the use of infringing material in cases where ... the plaintiff has made a strong showing of likely success on the merits." *Sun*, 188 F.3d at 1119 (citing *Cadence*, 125 F.3d at 830 (internal quotations omitted)).

However, because of the passage of time, the governing law has changed. Now, a plaintiff is not granted the presumption of irreparable harm upon a showing of likelihood of

success on the merits. Instead, a plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest. *Winter v. Natural Resources Defense Council*, 129 S. Ct. 365, 374 (2008) (citations omitted). In this recent case, the Supreme Court found that the Ninth Circuit's standard of the likelihood of irreparable injury was too lenient and held that a plaintiff must demonstrate that irreparable injury is "*likely* in the absence of an injunction." *Id*. at 375. "Issuing a preliminary injunction based only a possibility of irreparable harm is inconsistent with our characterization of injunctive relief as an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Id.* at 375-76 (citing *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997) (*per curiam*)). Because a preliminary injunction is an extraordinary remedy, "[i]n each case, courts 'must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief.' *Id*. at 376 (citing *Amoco Production Co. v. Gambell*, 480 U.S. 531, 542 (1987)). "'In exercising their sound discretion, courts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction.'" *Id.* at 376-77 (citing *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 312 (1982)).

2. Procedural History.

Plaintiff appealed this Court's denial of his original motion for preliminary injunction on the issue of copyright infringement. The Federal Circuit court found that this Court had erred in its legal finding that a copyright holder of work open and available to the public free of charge under an "open source" nonexclusive copyright license may not control future distribution and modification of such work under federal copyright law, but may only pursue remedies under a breach of contract theory. The Federal Circuit court found that Jacobsen may maintain a cause of action for trademark infringement based on the facts alleged in the complaint. In its decision, the appellate court found that copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material and that the Artistic License present on the JMRI Project website governed Jacobsen's copyrighted material and

required that any downstream user follow the restrictive terms of the license. Because the Federal Circuit found that this Court had erred in its legal finding, and, having found that the terms of the Artistic License are enforceable copyright conditions, the court vacated the denial of a preliminary injunction and remanded "to enable the District Court to determine whether Jacobsen has demonstrated (1) a likelihood of success on the merits and either a presumption of irreparable harm or a demonstration of irreparable harm; or (2) a fair chance of success on the merits and a clear disparity in the relative hardships and tipping in his favor." *Jacobsen v. Katzer*, 535 F.3d at 1382-83.

The Federal Circuit was faced with an incomplete record and only the allegations in the complaint, and made its determination as a matter of legal interpretation. The appellate court did not make a finding that Jacobsen is entitled to a preliminary injunction on the allegations of his complaint. It only found that this Court erred in finding that a cause of action for trademark infringement could not lie. This Court is again faced with a perfunctory record and is bound by the legal finding of the appellate decision. However, in the intervening time, the Supreme Court precedent governing the standard to be applied in deciding whether the extraordinary remedy of a preliminary injunction is appropriate has changed. This Court is bound by such intervening authority. In order to grant Jacobsen a preliminary injunction, the Court must find, based on the entire record, that Jacobsen is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest. *Winter*, 129 S. Ct. at 374.

3. Jacobsen Fails to Meet Heightened Burden of Demonstrating Harm.

In its opinion, the Federal Circuit found that in the open source field, there are potential harms to copyright holders, although they may not be exclusively monetary. The court found that the

> lack of money changing hands in open source licensing should not be presumed to mean that there is no economic consideration, however. There are substantial benefits, including economic benefits, to the creation and distribution of copyrighted works under public licenses that range far beyond traditional license royalties. For example, program creators may generate market share for their programs by providing certain components free of charge. Similarly, a programmer or company may increase its international reputation by incubating

> open source projects. Improvement to a product can come rapidly and free of charge from an expert not even known to the copyright holder.

Jacobsen v. Katzer, 535 F.3d at 1379. On this basis, the court found that there could indeed be harm based exclusively on a copyright infringement theory.

However, the Federal Circuit did not find, based on the record of this case, that there was indeed either actual, current infringement or that there was a likelihood of irreparable harm that tipped the balance of equities in Jacobsen's favor. The Federal Circuit court's list of potential harms that a copyright holder may face in the open source field are just that – *potential* harms. There is no showing on the record before this Court that Jacobsen has actually suffered *any* of these potential harms. The standard under *Winter* requires that Jacobsen demonstrate, by the introduction of admissible evidence and with a clear likelihood of success that the harm is real, imminent and significant, not just speculative or potential. 129 S. Ct. at 374. Jacobsen has failed to proffer any evidence of any specific and actual harm suffered as a result of the alleged copyright infringement and he has failed to demonstrate that there is any continuing or ongoing conduct that indicates future harm is imminent.[3] Because Jacobsen fails to meet the burden of presenting evidence of actual injury to support his claims of irreparable injury and speculative losses, the Court cannot, on this record, grant a preliminary injunction. *See Goldie's Bookstore, Inc. v. Superior Court*, 739 F.2d 466, 472 (9th Cir. 1984) (holding that speculative harm is insufficient to establish irreparable harm).

[3] Although Jacobsen makes legal arguments regarding the alleged harm he may suffer, for instance delays and inefficiency in development and time lost in the open source development cycle, he has failed to put forward any *evidence* of such harms. Jacobsen has failed to proffer evidence of harm suffered or any evidence of a real or immediate threat of imminent harm in the future. The Court also finds that Jacobsen has failed to identify with the requisite particularity the extent of his copyright ownership over the disputed underlying material. The JMRI Project Decoder Definition Files incorporate many manufacturers' specifications data as well as rights to specific terms whose copyright is owned by Defendants. Even if Jacobsen's heavy burden to warrant injunctive relief had been met, it is unclear how the Court would fashion an injunction which would be narrowly tailored to enjoin only those allegedly infringing uses of Jacobsen's copyrighted content.

CONCLUSION

For the foregoing reasons, the Court GRANTS Defendants' motion to dismiss for mootness; GRANTS IN PART AND DENIES IN PART Defendants' motion to dismiss for failure to state a claim; DENIES the motion to strike; and DENIES Jacobsen's motion for preliminary injunction. Jacobsen may file an amended complaint within twenty days of the date of this Order. If Jacobsen does not file a third amended complaint, Defendants shall file an answer within twenty days of the deadline to file the amended complaint. If Jacobsen elects to file a third amended complaint in accordance with this Order, Defendants shall either file an answer or move to dismiss within twenty days of service of the third amended complaint.

IT IS SO ORDERED.

Dated: January 5, 2009

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION, a Washington Corporation, Plaintiff, v. TOMTOM N.V., a Netherlands Corporation, and TOMTOM, INC., a Massachusetts Corporation, Defendants.	Case No: _____ **COMPLAINT FOR PATENT INFRINGEMENT** **JURY DEMAND**

Plaintiff Microsoft Corporation ("Microsoft") for its Complaint For Patent Infringement against Defendants TomTom N.V. and TomTom, Inc. (collectively, the "Defendants"), alleges as follows:

PARTIES

1. Plaintiff Microsoft Corporation is a Washington corporation having its principal place of business at One Microsoft Way, Redmond, Washington 98052.

2. Founded in 1975, Microsoft is a worldwide leader in computer software, services and solutions for businesses and consumers. Since 1979, Microsoft has been headquartered in the Seattle, Washington metropolitan area, currently employs more than 20,000 people in the Seattle area, and occupies nearly 8 million square feet of facilities at its Redmond campus.

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

3. Microsoft has a long history of technical innovation in the software and hardware products it develops and distributes. These software products include operating systems for servers, personal computers, embedded devices, smartphones, PDAs, and other intelligent devices; server applications for distributed computing environments; information worker productivity applications; business solution applications; high-performance computing applications; software development tools; operating systems for automotive applications; and various navigation-related software products and services.

4. Upon information and belief, Defendant TomTom N.V. is a Dutch corporation organized and existing under the laws of the Netherlands having a principal place of business at Rembrandtplein 35, Amsterdam 1017 CT, Netherlands.

5. Upon information and belief, Defendant TomTom, Inc. is a corporation organized and existing under the laws of Massachusetts and is a wholly-owned subsidiary of TomTom N.V. TomTom, Inc.'s principal place of business is located at 150 Baker Ave Ext., Concord, Massachusetts 01742.

6. Upon information and belief, Defendants are in the business of developing, manufacturing, and selling portable navigation computing devices and software for use on those devices, personal computers, PDAs, and smartphones (hereinafter known collectively as "Portable Navigation Devices and Software"). Upon information and belief, Defendants market and distribute their products worldwide, including in the United States, through their channel business partners and various retail companies, at retail stores, through the websites of retail companies, and on their own websites. Upon information and belief, Defendants do business within the Western District of Washington.

JURISDICTION AND VENUE

7. This is an action for patent infringement arising under the patent laws of the United States, Title 35, United States Code.

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

9. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b), 1391(c) and 1400(b). On information and belief, Defendants are subject to this Court's personal jurisdiction, consistent with the principles of due process and the Washington Long Arm Statute, because each Defendant offers for sale and sells Portable Navigation Devices and Software in the Western District of Washington, has transacted business in this District, and/or has committed and/or induced acts of patent infringement in this District. For example, Defendants' own website (e.g., http://www.tomtom.com/page/giftguide?Lid=4&selector=true) allows users to purchase Defendants' products for delivery within this District. The website at http://www.tomtom.com/stores/type.php?ID=2&Country=223 directs users of the Defendants' website to retail outlets selling Defendants' products within this District. Additionally, the website at http://www.tomtom.com/stores/type.php?ID=1&Country=223 directs users of the Defendants' website to online merchants selling Defendants' products for delivery within this District.

PATENT INFRINGEMENT COUNTS

10. Microsoft is the owner of all right, title, and interest in U.S. Patent Nos. 6,175,789; 7,054,745; 6,704,032; 7,117,286; 6,202,008; 5,579,517; 5,758,352; and 6,256,642 (collectively, "the Microsoft patents-in-suit"), which the Defendants are directly infringing and/or inducing others to infringe by making, using, offering to sell or selling in the United States, or importing into the United States, products or processes that practice inventions claimed in the Microsoft patents-in-suit.

11. The Defendants have profited through infringement of the Microsoft patents-in-suit. As a result of the Defendants' unlawful infringement of the Microsoft patents-in-suit patent, Microsoft has suffered and will continue to suffer damage. Microsoft is entitled to

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

recover from the Defendants the damages suffered by Microsoft as a result of the Defendants' unlawful acts.

12. Defendants' infringement of the Microsoft patents-in-suit constitutes willful and deliberate infringement, entitling Microsoft to enhanced damages and reasonable attorney fees and costs. Microsoft provided defendant TomTom N.V. notice of its infringement allegations in a June 13, 2008 letter to Peter-Frans Pauwels, Chief Technical Officer of Defendant TomTom N.V. Upon information and belief, Defendant TomTom, Inc. received notice of Microsoft's infringement allegations from its parent, TomTom N.V.

13. Upon information and belief, the Defendants intend to continue their unlawful infringing activity, and Microsoft continues to and will continue to suffer irreparable harm—for which there is no adequate remedy at law—from such unlawful infringing activity unless Defendants are enjoined by this Court.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 6,175,789

14. Microsoft realleges and incorporates by reference the allegations set forth in paragraphs 1-13.

15. Microsoft is the owner of all right, title, and interest in U.S. Patent No. 6,175,789 ("the '789 patent"), entitled "Vehicle Computer System with Open Platform Architecture" duly and properly issued by the U.S. Patent and Trademark Office on January 16, 2001. A copy of the '789 patent is attached as Exhibit A.

16. The Defendants have been and/or are directly infringing and/or inducing others to infringe the '789 patent by, among other things, making, using, offering to sell or selling in the United States, or importing into the United States, products, including various Portable Navigation Devices and Software that embody or incorporate, or the operation of which otherwise practices, one or more claims of the '789 patent.

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 7,054,745

17. Microsoft realleges and incorporates by reference the allegations set forth in paragraphs 1-13.

18. Microsoft is the owner of all right, title, and interest in U.S. Patent No. 7,054,745 ("the '745 patent"), entitled "Method and System For Generating Driving Directions," duly and properly issued by the U.S. Patent and Trademark Office on May 30, 2006. A copy of the '745 patent is attached as Exhibit B.

19. The Defendants have been and/or are directly infringing and/or inducing others to infringe the '745 patent by, among other things, making, using, offering to sell or selling in the United States, or importing into the United States, products, including various Portable Navigation Devices and Software that embody or incorporate, or the operation of which otherwise practices, one or more claims of the '745 patent.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 6,704,032

20. Microsoft realleges and incorporates by reference the allegations set forth in paragraphs 1-13.

21. Microsoft is the owner of all right, title, and interest in U.S. Patent No. 6,704,032 ("the '032 patent"), entitled "Methods and Arrangements for Interacting with Controllable Objects within a Graphical User Interface Environment Using Various Input Mechanisms," duly and properly issued by the U.S. Patent and Trademark Office on March 9, 2004. A copy of the '032 patent is attached as Exhibit C.

22. The Defendants have been and/or are directly infringing and/or inducing others to infringe the '032 patent by, among other things, making, using, offering to sell or selling in the United States, or importing into the United States, products, including various Portable

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

Navigation Devices and Software that embody or incorporate, or the operation of which otherwise practices, one or more claims of the '032 patent.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 7,117,286

23. Microsoft realleges and incorporates by reference the allegations set forth in paragraphs 1-13.

24. Microsoft is the owner of all right, title, and interest in U.S. Patent No. 7,117,286 ("the '286 patent"), entitled "Portable Computing Device-integrated Appliance," duly and properly issued by the U.S. Patent and Trademark Office on October 3, 2006. A copy of the '286 patent is attached as Exhibit D.

25. The Defendants have been and/or are directly infringing and/or inducing others to infringe the '286 patent by, among other things, making, using, offering to sell or selling in the United States, or importing into the United States, products, including various Portable Navigation Devices and Software that embody or incorporate, or the operation of which otherwise practices, one or more claims of the '286 patent.

COUNT V

INFRINGEMENT OF U.S. PATENT NO. 6,202,008

26. Microsoft realleges and incorporates by reference the allegations set forth in paragraphs 1-13.

27. Microsoft is the owner of all right, title, and interest in U.S. Patent No. 6,202,008 ("the '008 patent"), entitled "Vehicle Computer System with Wireless Internet Connectivity," duly and properly issued by the U.S. Patent and Trademark Office on March 13, 2001. A copy of the '008 patent is attached as Exhibit E.

28. The Defendants have been and/or are directly infringing and/or inducing others to infringe the '008 patent by, among other things, making, using, offering to sell or selling in the United States, or importing into the United States, products, including various Portable

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

Navigation Devices and Software that embody or incorporate, or the operation of which otherwise practices, one or more claims of the '008 patent.

COUNT VI

INFRINGEMENT OF U.S. PATENT NO. 5,579,517

29. Microsoft realleges and incorporates by reference the allegations set forth in paragraphs 1-13.

30. Microsoft is the owner of all right, title, and interest in U.S. Patent No. 5,579,517 ("the '517 patent"), entitled "Common Name Space for Long and Short Filenames," duly and properly issued by the U.S. Patent and Trademark Office on November 26, 1996. A reexamination certificate was issued by the U.S. Patent and Trademark Office for the '517 patent on November 28, 2006. A copy of the '517 patent, including reexamination certificate, is attached as Exhibit F.

31. The Defendants have been and/or are directly infringing and/or inducing others to infringe the '517 patent by, among other things, making, using, offering to sell or selling in the United States, or importing into the United States, products, including various Portable Navigation Devices and Software that embody or incorporate, or the operation of which otherwise practices, one or more claims of the '517 patent.

COUNT VII

INFRINGEMENT OF U.S. PATENT NO. 5,758,352

32. Microsoft realleges and incorporates by reference the allegations set forth in paragraphs 1-13.

33. Microsoft is the owner of all right, title, and interest in U.S. Patent No. 5,758,352 ("the '352 patent"), entitled "Common Name Space for Long and Short Filenames," duly and properly issued by the U.S. Patent and Trademark Office on May 26, 1998. A reexamination certificate was issued by the U.S. Patent and Trademark Office for the '352 patent on October

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

10, 2006. A copy of the '352 patent, including reexamination certificate, is attached as Exhibit G.

34. The Defendants have been and/or are directly infringing and/or inducing others to infringe the '352 patent by, among other things, making, using, offering to sell or selling in the United States, or importing into the United States, products, including various Portable Navigation Devices and Software that embody or incorporate, or the operation of which otherwise practices, one or more claims of the '352 patent.

COUNT VIII

INFRINGEMENT OF U.S. PATENT NO. 6,256,642

35. Microsoft realleges and incorporates by reference the allegations set forth in paragraphs 1-13.

36. Microsoft is the owner of all right, title, and interest in U.S. Patent No. 6,256,642 ("the '642 patent"), entitled "Method and System for File System Management Using a Flash-Erasable, Programmable, Read-only Memory" duly and properly issued by the U.S. Patent and Trademark Office on July 3, 2001. A copy of the '642 patent is attached as Exhibit H.

37. The Defendants have been and/or are directly infringing and/or inducing others to infringe the '642 patent by, among other things, making, using, offering to sell or selling in the United States, or importing into the United States, products, including various Portable Navigation Devices and Software that embody or incorporate, or the operation of which otherwise practices, one or more claims of the '642 patent.

DEMAND FOR JURY TRIAL

38. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Microsoft respectfully requests a trial by jury on all issues properly triable by jury.

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for relief as follows:

A. For a judgment declaring that each Defendant has infringed at least one claim of each of the Microsoft patents-in-suit;

B. For a judgment awarding Microsoft compensatory damages as a result of each Defendant's infringement of the Microsoft patents-in-suit, together with interest and costs, and in no event less than a reasonable royalty;

C. For a judgment declaring that each Defendant's infringement of the Microsoft patents-in-suit, has been willful and deliberate;

D. For a judgment awarding Microsoft treble damages and pre-judgment interest under 35 U.S.C. § 284 as a result of each Defendant's willful and deliberate infringement of the Microsoft patents-in-suit;

E. For a judgment declaring that this case is exceptional as to each Defendant and awarding Microsoft its expenses, costs, and attorneys fees in accordance with 35 U.S.C. §§ 284 and 285 and Rule 54(d) of the Federal Rules of Civil Procedure;

F. For a grant of permanent injunction pursuant to 35 U.S.C. § 283, enjoining each Defendant from further acts of infringement; and

G. For such other and further relief as the Court deems just and proper.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

Dated: February 25, 2009

By: s/ Adam R. Wichman

Adam R. Wichman (WSBA No. 38466)
adam.wichman@klarquist.com
John D. Vandenberg (WSBA No. 38445)
john.vandenberg@klarquist.com
600 University Street, Suite 2950
Seattle, WA 98101
Telephone: 206-264-2960
Facsimile: 206-624-2719

OF COUNSEL:

David E. Killough (WSBA No. 40185)
davkill@microsoft.com
MICROSOFT CORPORATION
One Microsoft Way, 8/2076
Redmond, WA 98052
Telephone: 425-703-8865
Facsimile: 425-869-1327

David T. Pritikin
dpritikin@sidley.com
Richard A. Cederoth
rcederoth@sidley.com
Douglas I. Lewis
dilewis@sidley.com
John W. McBride
jwmcbride@sidley.com
SIDLEY AUSTIN LLP
One South Dearborn
Chicago, IL 60603
Telephone: 312-853-7000
Facsimile: 312-853-7036

Marc R. Ascolese
mascolese@sidley.com
SIDLEY AUSTIN LLP
555 California Street, Suite 2000
San Francisco, CA 94104-1715
Telephone: 415-772-1200
Facsimile: 415-772-7400

Attorneys for Plaintiff
MICROSOFT CORPORATION

KLARQUIST SPARKMAN, LLP
One Union Square
600 University Street, Suite 2950
Seattle, WA 98101
(206) 264-2960

Legislative and Regulatory Update –

How Washington's Concerns with Privacy and Data Security Impact Your Business

What Should You Do About It?

March 31, 2009
Los Angeles, CA
Paul Martino

ALSTON+BIRD LLP

2 Key Issue Areas

- **Online Behavioral Targeting**
  - Is Government "Crying Wolf" or Is This a "Wake-Up" Call?
  - Overview of Latest FTC Staff Report *(Released Feb. 2009)*
  - Recent Remarks of Key Washington Policy Makers
  - Industry's Policy Response
  - Steps for Companies to Consider
- **Other Privacy and Data Security Legislation**
  - Personal Health Information: ARRA Significantly Revises HIPAA
  - Comprehensive Federal Privacy Legislation
  - Federal Data Security Legislation Gives Way to States

ALSTON+BIRD LLP

Online Behavioral Targeting (OBT)

- **This is Industry's Wake-Up Call**
  - New FTC Chairman Leibowitz Means Business About OBT...
  - And So Does Senate and House Commerce Committees...
  - IF Industry Doesn't Act Convincingly to Assuage Their Concerns
- **But Can Self Regulation Work?**
  - An Unsure U.S. Government is Applying Pressure to Industry
    - FTC Town Hall (11/07), OBT Principles (12/07), Staff Report (2/09)
    - Senate and House Hearings (Summer/Fall 2008; More Planned)
  - Industry is Engaged in Various Efforts to Create Best Practices
  - What If Industry's Framework Does Not Work?

ALSTON+BIRD LLP

Overview of FTC Staff Report on OBT

- **Scope of the FTC Principles**
  - "Any data [PII or Non-PII] collected for online behavioral advertising that reasonably could be associated with a particular consumer or with a particular computer or device"
  - 2 Types of Online Advertising Excluded from Definition of OBT
    - "First Party Advertising" (Site to Customer; No 3rd Party Data Sharing)
    - "Contextual Advertising" (Ad Based on Single Site Visit/Search Query)
- **The 4 Principles**
  - Transparency & Consumer Control ("Prominent" Notice/Opt-Out)
  - Reasonable Security and Limited Data Retention
  - Opt-In for Material Changes to Existing Privacy Promises
  - Opt-In for Use of "Sensitive" Data (Undefined)

ALSTON+BIRD LLP

Recent Remarks of FTC Chairman

- **FTC Chairman Leibowitz**
  - Industry is not protecting consumer privacy interests related to OBT
  - The FTC principles are a guide to improving the online environment
  - Industry should adopt self-regulatory policies similar to the FTC principles...and do it soon
  - A self-regulatory regime can be the fastest way to get the changes needed online to better protect consumers' privacy interests but...
  - If industry does not improve these practices, the FTC and Congress will move to a more regulatory model for behavioral advertising

Recent Remarks of House Telecom Chairman

- **House Telecom Subcmte. Chairman Boucher (D-VA)**
  - The subcommittee held hearings and legislation may be necessary
  - Behavioral advertising is another in a line of data privacy issues
  - A few key principles being considered for possible legislation:
    - All websites must have a privacy policy
    - A website collecting "any" data from a consumer must conspicuously provide notice of what data is collected and how that data may be used
    - If the data is to be used for marketing, the site must provide an opt-out
    - Sharing data with "unaffiliated" 3rd parties should be prohibited without first obtaining an Internet users' affirmative consent (i.e., an opt-in)

Industry's Policy Response in Washington

- **Self-Regulatory Efforts**
  - Efforts to Develop Industry Standard Guidelines and Principles
  - Re-Examination of Opt-Out Cookies and Technology
  - Discussion of Creative New Procedures for Advertising Notices
- **Legislative and Regulatory Policy Campaigns**
  - Submission of Comments (Formal & Informal) to FTC Principles
  - Lobbying Key Committees and Members of Congress on Bills
  - Formation of "Consumer-Focused" Business Forums
  - While Bill Passage Unlikely This Year, Negative Media Looms

ALSTON+BIRD LLP

Steps for Companies to Consider

- **Meet Internally to Review Current Online Ad Practices**
  - Prominence of Notice and Clarity of Choice Offered to Consumers
  - Pay Special Attention to Any Use of Sensitive Data
  - Consider Appropriate Data Security and Retention Practices
  - Determine Triggers for Material Changes to Consumer Privacy Promises
- **Assess Regulatory and Legislative Risk**
  - Analyze Potential Impact to Business Practices of Current Proposals
  - Determine Corporate Priorities and Flexibility to Change Ad Models
- **Actively Monitor *but also* Consider a Policy Campaign**
  - Make Use of Washington Office and Outside Resources for Information
  - Join Appropriate Groups to Form Strategic Public Policy Alliances
  - Effectively "Shaping" Policy Now Helps Reduce Business Costs Later

ALSTON+BIRD LLP

Effective Public Policy Campaigns

- **Effectively Addressing Regulatory Proposals Can...**
  - Reduce potential impact on existing or future advertising models
  - Minimize regulatory risk to business and expanded liability
  - Increase business certainty in value of investing in greater range of targeted online advertising practices to win more customers
- **Compliance with Self-Regulatory Standards Can...**
  - Assure customers that your advertising practices are consumer-friendly and consistent with best business practices
  - Avoid the greater cost, rigidity and uncertainty of regulatory regimes

ALSTON+BIRD LLP

Other Privacy and Data Security Issues

- **Personal Health Information (PHI)**
  - ARRA Significantly Revises HIPAA Privacy and Security Rules
  - Compliance Required by February 2010
- **Comprehensive Federal Privacy Legislation**
  - Will This Be the Congress That Finally Does It?
  - *Probably Not.*
- **Federal Data Security Legislation Gets Less Likely**
  - Approach Balkanized – First the Vets, Now HIPAA, What's Next?
  - State Data Security Breach Laws Continue to Evolve

ALSTON+BIRD LLP

Personal Health Information (PHI): New Privacy and Data Security Rules

- **ARRA Significantly Revises HIPAA Rules**
  - American Recovery and Reinvestment Act of 2009 ("ARRA") Amends Privacy and Security Rules under Health Information Portability and Accounting Act of 1996 ("HIPAA Rules")
    - President Obama signed into law on February 17, 2009
    - One Year for Companies to Come Into Compliance with New Rules
- **Four Significant Changes**
  - Broader Application to Business Associates, Vendors of Personal Health Records (PHRs) & Other Non-HIPAA-Covered Entities
  - Statutory Security Breach Notification Requirements for PHI
  - New Patient Protections for Electronic Health Records (EHRs)
  - Expanded Civil Enforcement including State AG Actions

Comprehensive Federal Privacy Legislation: Continued Calls Go Unanswered

- **Privacy is a Complicated Statutory Issue**
  - Few members of Congress understand it in depth
  - Difficult for staff to draft carefully tailored definitions and provisions
- **"One-Size-Fits-All" Legislation Rarely Fits Any One**
  - U.S. has had a Sector-Specific Approach to Privacy Protections
  - Creation of a Harmonized Overlay Raises Questions of Necessity
- **Congress Continues to Bite Off Smaller Chunks**
  - ARRA Amends HIPAA Privacy and Security Rules
  - Financial Services Regulatory Restructuring? *Watch Out, Folks!*

Federal Data Security Legislation: Effort at Federal Law Gives Way to States

- **Well-Publicized Data Security Breaches Had Effect**
  - Negative media attention harmful to brands and customer retention
  - Industry practices and systems technology improved as a result
- **Businesses Understand Data Security and Improving**
  - Protecting business data is understandable and achievable objective
  - Increasing prevalence across businesses of CSOs and CISOs
  - Still some "bad apples" out there
- **State Data Security Breach Notification Laws**
  - Many states first followed California's law and compliance was not difficult
  - Industry call for federal law preemptive of state laws waned over last 4 yrs
  - However, some states are getting more aggressive with legislation
  - Could this be the start of new calls for a federal bill? *We'll see...*

ALSTON+BIRD LLP

THANK YOU!

- **Contact Information:**

Paul Martino
Alston & Bird LLP
950 F Street, NW
Washington, DC 20004
(202) 756-3439
paul.martino@alston.com

- **Biography:**

http://www.alston.com/paul_martino

ALSTON+BIRD LLP

Supporting Materials

Health Care Advisory

American Recovery and Reinvestment Act of 2009: Privacy and Security Provisions "Up the Ante" for Covered Entities, Business Associates and Non-Covered HIPAA Entities

March 3, 2009

http://www.alston.com/files/Publication/73254df7-2e6d-4c31-a6a5-3d4991819521/Presentation/PublicationAttachment/634e7eb8-3e64-4061-adc6-3fe1c3918499/ARRA%20Act%20of%202009.pdf

If you would like to receive future *Health Care Advisories* electronically, please forward your contact information including e-mail address to **healthcare.advisory@alston.com**. Be sure to put "**subscribe**" in the subject line.

Privacy & Security Task Force ADVISORY

States Adopting Aggressive New Privacy and Data Security Laws and Regulations

October 7, 2008

http://www.alston.com/files/Publication/05c1737d-ccfc-44a2-9252-1ffbea8953d3/Presentation/PublicationAttachment/a5a0be6c-e8c5-4b3c-ad17-134c3b6f0cd6/Privacy%20Post%20Vol%204.pdf

If you would like to receive future *Privacy & Security Task Force Advisories* electronically, please forward your contact information including e-mail address to **Privacy.Post@alston.com.** Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of our **Privacy & Security Task Force** attorneys.

Intellectual Property/Legislative ADVISORY

Patent Reform Act of 2009 Introduced in Senate and House; Senate Judiciary Committee Holds First Hearing

March 13, 2009

http://www.alston.com/files/Publication/6f0a5842-86f0-4486-be9e-0218cb5623cf/Presentation/PublicationAttachment/f4893e93-bcde-45b7-9d8f-508a07c5143a/Patent%20Act%20of%202009.pdf

If you would like to receive future *Intellectual Property /Energy Advisories* electronically, please forward your contact information including e-mail address to **ip.advisory@alston.com**. Be sure to put "**subscribe**" in the subject line.

Outlook for the 111th Congress & President-elect Barack Obama

November 6, 2008 11:54 AM

http://www.alston.com/files/Publication/201d90a9-aec6-48fe-b27b-5a63cd00f28d/Presentation/PublicationAttachment/396476ac-b2bf-47d6-a4ad-981e118bacfa/Post%20Election%20Advisory.pdf

If you would like to receive future *Legislative & Public Policy Advisories* electronically, please forward your contact information including e-mail address to **legislative.advisory@alston.com**. Be sure to put "**subscribe**" in the subject line.

Botnets, Pirates, and Cybercriminals

What are the current trends??

Mark Ishikawa
March 31, 2009
Los Angeles, CA

Scope of Online Intellectual Property Piracy

- Estimated 60 million people using file sharing applications worldwide at any given time
- Available content includes movies, TV shows, music, software, video games, audio books
- BayTSP finds 16 million to 18 million infringements of client intellectual property online daily and sends more than 1 million takedown notices monthly.

Downloading as easy as using Google

Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100

Pirate Search

All Audio Video Applications Games Other (search titles only)

Browse Torrents

Audio
Music, Audio books, Sound clips, FLAC, Other

Video
Movies, Movies DVDR, Music videos, Movie clips, TV shows, Handheld, Highres - Movies, Highres - TV shows, Other

Applications
Windows, Mac, UNIX, Handheld, Other OS

Games
PC, Mac, PS2, XBOX360, Wii, Handheld, Other

Other
E-books, Comics, Pictures, Covers, Other

Business Software often infected with malware and spyware

Type	Name	Uploaded	Size	SE	LE
Applications > Windows	WinRAR_3.80_Professional	11-13 2008	1.25 MiB	2058	16
Applications > Windows	Adobe Photoshop CS4 Extended [clean][blaze69] 7z	02-20 18:10	891.35 MiB	2030	498
Applications > Windows	Adobe CS4 Master Collection(Purchased from Adobe.com)-Shadeyman	12-19 2008	5.43 GiB	1727	3508
Applications > Windows	Microsoft Office 2007 Enterprise Edition [blaze69]	02-20 07:25	558.85 MiB	1649	229
Applications > Windows	Windows 7 build 7057 x86	03-12 01:44	2.51 GiB	1526	1574
Applications > Windows	Adobe Photoshop CS3 Extended + Crack	01-08 2008	568.4 MiB	1341	163
Applications > Windows	Nero 7.10.1.0	07-28 2007	173.64 MiB	1336	51
Applications > Windows	Nero 9.0.9.4b (ahead nero) Full install + patch	03-20 14:42	592.06 MiB	1306	537
Applications > Windows	AVG Antivirus 8 0 + serial (EXPIRES YEAR 2018) (CLEAN) [blaze69]	02-20 04:28	59.46 MiB	1219	81
Applications > Windows	WINDOWS XP SP3 2009 ULTRA EDITION	12-30 2008	688.89 MiB	1143	286

Popular Music Packaged With Malware

Quick Response Needed to Contain IP leaks

Emergency RADAR - BayTSP's quick response team

- Monitors all major Internet protocols
- Identifies and tracks client assets and immediately notifies client once the leak has been validated.
- Options for high priority scanning, detection logs, takedown notices, reporting and detailed evidence collection for possible litigation.

Case Study - Intellectual Property Leak

- Major software company
- Code for highly anticipated software application leaked to the Internet
- Within hours more than 60,000 people were downloading
- Reduced to 600 within one week

ALSTON+BIRD LLP

Thank you!

Mark Ishikawa
BayTSP, Inc.
P.O. Box 1314
Los Gatos, CA 95031
408.341.2300 - phone
408.341.2399 - fax

marki@baytsp.com

http://www.baytsp.com

ALSTON+BIRD LLP

Information Security Policy

Threats
Response
Enforcement

Michael Zweiback
Los Angeles Office

March 31, 2009
Los Angeles, CA

Threats In The "Wild"

- State Sponsored - Russian Business Network
- Highly Sophisticated Organized Profiteers
  - Botnet operators and Malware writers who share work through chat channels;
  - Extortion via hacking-Express Scripts Investigation - Threat to publish hacked HIPAA (including SSNs) information detailed in PC World.
- Disgruntled Employees - Vendors/Contract IT
- Hacktivists - Bragging Rights - University Hacking - USC

- BotNETs are the growing underworld infrastructure for web disruption and criminal activity.
  - Distributed Denial of Service (DDOS)- Generally for purposes of extortion.
  - Spreading Infection/malware
  - E-Mail SPAM- Most spam is distributed by BotNET

ALSTON+BIRD LLP

ALSTON+BIRD LLP

Development Of An Information Security Plan

- Do you know what you have and why you keep it?
- Have you segregated access so that only those who need sensitive information have access? Where are your Trade Secrets?
- Have you clearly designated responsibilities in the event of a security breach?
- If the effected technology platform is outsourced how do you obtain access? What are your access rights?

How Do You Respond?

- So you get the 3:00 a.m. call- Are you ready to act?
- Do you have a response plan? Who do you need?
- Start small and build out;
- IT Staff are your first responders;
- Chief Information Privacy Officer – Coordination;
- HR- if the breach is internal what are the existing privacy policies that impact your ability to obtain information;

- General Counsel's Role- Quarterback
  - To communicate with C-level executives
  - Insure resources properly allocated and available
  - Coordinate press response, if necessary
- Outside Counsel Role
  - Breach notification requirements
  - Timing - Safe harbors for law enforcement
  - If multiple jurisdictions impacted you need to know the laws of each state as well as international jurisdictions.
  - Are you going to need to self-report the incident to regulators?

The Regulators

Federal Trade Commission Enforcement under Section 5 of the FTC

- Prohibits unfair or deceptive promises in privacy statements including promises about the security of consumers personal information.
  - FTC v. GUIDANCE SOFTWARE
- Unfairness authority to challenge information practices that cause substantial consumer injury
  - FTC v. TJ MAXX

- Penalties for a violation can include:
  - Establish comprehensive security program;
  - Audit every two years by a third party;
  - Reporting to the FTC;
  - If breach demonstrates compliance is seriously lacking, outside monitor may be required;
  - Under regulatory scrutiny for 10-20 years - similar to an injunction.

Others Are Also Watching-

- SEC now enforcing “Safeguards Rule” of federal securities laws for broker-dealers and SEC registered investment advisors.
- SEC v. LPL Financial- Sept.11, 2008 -Failure to adopt policies to safeguard customer information – 10,000 customers vulnerable after hacking of online trading platform.

Others Are Also Watching-

- SEC Penalties-
  - Cease and desist from future violations of Safeguards Rule;
  - $275,000 fine;
  - Must retain independent expert to review policies and procedures;
  - Implement a policy and set procedures for training employees to safeguard customer data.

ALSTON+BIRD LLP

You Are Not Done

- FTC-COPA-Sony BMG - Largest FTC Settlement Ever
- Health and Human Services-
  - Providence Health Services - Stolen medical records as a result of lost lap tops; Paid $100,000 Fine to DOJ
- State Attorneys General -Texas and California very active-enforcement of federal regulatory schemes;
- Increasing Class Action Litigation- Erosion of Actual Damages requirement

ALSTON+BIRD LLP

Intellectual Property Practice

Overview

Intellectual property issues are often at the core of competition in today's rapidly expanding world market. U.S. and foreign patent protection. Patent, trademark, trade secret and copyright litigation. The Internet. Technology and merchandise licensing. Worldwide trademark registration and protection. Outsourcing and its attendant concerns. These issues and others define not just profitability but survival.

To make sure your company's intellectual property is protected in the U.S. and abroad, you need a law firm that has extensive experience in all areas of intellectual property law and a full range of capabilities to handle any issue that may arise. Alston & Bird is that law firm. Alston & Bird attorneys draw on more than 85 years of commitment to intellectual property as a specialty practice. Numbering over 180 lawyers, including more than 120 legal professionals registered to practice before the U.S. Patent and Trademark office and fifteen with Ph.D's. Alston & Bird's Intellectual Property group is one of the largest in any general practice firm in the country.

Depth and Experience

The Intellectual Property Group of Alston & Bird provides a full-range of intellectual property services including:

- Patent preparation and prosecution in emerging technologies such as genetic engineering and hybridoma technology, chip and mask technology and computer technology, as well as the traditional areas of electronics, mechanical, chemical and biotechnology matters. We regularly file about 1,300 U.S. and 1,000 foreign patent applications each year.
- We have one of the largest and deepest intellectual property litigation practices, with jury and non-jury experience in U.S. patent, trademark, copyright, trade secret, false advertising and anti-counterfeiting litigation, as well as access to Alston & Bird's substantial depth and expertise in related antitrust matters; and substantial experience in coordinating multinational intellectual property litigation programs. We have obtained eight-figure jury verdicts for plaintiffs and summary judgment victories for defendants.
- Trademark and domain name clearance, registration and portfolio management both domestically and worldwide, including over 24,000 registrations for hundreds of clients in more than 200 jurisdictions. We also protect these rights when necessary in enforcement, opposition and cancellation proceedings.
- Transactional expertise in licensing, sponsorship and merchandising matters and information technology transactions, with a core of lawyers focused on emerging IP issues related to electronic commerce and the Internet, including domain name

disputes, web-site and on-line development agreements, encryption technology, marketing and advertising.

Vision

More than just the skills to obtain a patent or trademark registration, Alston & Bird draws on 85 years of expertise to integrate these talents to build an effective and long term intellectual property program that will maximize your return on investment. This includes invention harvesting and assessment, portfolio management and mapping, marketing and branding strategies, out- and in-licensing of critical technology, and maintaining market exclusivity.

As you evaluate the skills necessary to best represent you, consider whether the firm is committed to providing the full range of legal and technical expertise to deal with the intellectual property issues. Alston & Bird certainly is. The strength and depth of our practice distinguishes Alston & Bird from any other general practice firm in the southeastern U.S. and provides the best evidence of Alston & Bird's commitment to this increasingly critical area of the law.

In today's market, you need a full-service intellectual property firm that can effectively bring every resource to bear for you anywhere in the world. Alston & Bird is the firm best positioned to help you protect your interests.

ALSTON+BIRD LLP

Intellectual Property Representative Clients

Aflac Incorporated

BASF Corporation

Belk Stores Services, Inc.

The Boeing Company

Coats plc

CommScope, Inc.

Dale Earnhardt, Inc.

The Estate of Bobby Jones

Georgia-Pacific Corporation

Celanese Ventures USA

Honeywell International Incorporated

Husqvarna USA

Invesco

Lance, Inc.

McKesson Corporation

Mohawk Industries

National Association for Stock Car Auto Racing, Inc. (NASCAR)

Nokia, Inc.

Paragon Trade Brands, Inc.

Rexam, Inc.

Scientific Atlanta, A Cisco Company

Sealed Air Corporation

Sonoco Products Company

Timberland

The TJX Companies, Inc.

Turner Broadcasting System, Inc.

Uniden America Corporation

UPS

VF Corporation

ALSTON+BIRD LLP

Jonathan M. Gordon
Alston & Bird LLP
333 South Hope Street
16th Floor
Los Angeles, CA 90071
213-576-1165
jonathan.gordon@alston.com

Services
Intellectual Property
IP & Technology Transactions

Education
Northwestern University
(J.D., 1978)

Claremont McKenna College
(B.A., 1974)

Admitted to Practice
California

Jonathan M. Gordon

Jonathan Gordon, partner in the firm's Los Angeles office, advises clients involved in the commercialization of new technologies, intellectual property and licensing transactions, and technology research and development. He counsels clients on their business transactions and practices over the Internet. Mr. Gordon also handles disputes involving licenses, patents, copyrights, trademarks and trade secrets, as well as other business disputes. He has represented clients in state and federal courts and in a variety of domestic and international arbitration forums.

Jonathan's clients include technology companies, emerging growth companies, individual inventors and founders, and Fortune 500 companies in business sectors including communications, software, life sciences, apparel and entertainment. He is experienced in advising clients on a wide range of alternative dispute resolution techniques, including mediations and arbitrations. Jonathan advises his colleagues on ethical issues and has written and lectured on professional ethics.

Jonathan is peer-review rated "AV" by LexisNexis Martindale-Hubbell and was recently named a Southern California "Super Lawyer" in the field of Intellectual Property by Law & Politics and the publishers of *Los Angeles Magazine*.

He received his J.D. from Northwestern University in 1978 and his B.A. from Claremont McKenna College in 1974.

Representative Experience

- Handles technology transfer and licensing transactions for commercialization of technologies including wireless sensor networks, detection systems, consumer and electronics products, optics, medical devices, software and nanotechnology.
- Represented Internet consumer business from early stage through successful sale of assets in connection with Internet transactions, advertising, data and IP issues.
- Successfully resolved multi-forum patent dispute involving two international arbitration proceedings and a final U.S. District Court judgment.
- Supervised copyright litigation and related remedies under the Digital Millennium Copyright Act on behalf of major motion picture studio to successfully stop unauthorized use and copying of content on the Internet.

- Handles licensing and IP transactions for global consumer goods company.
- Successfully represented software licensees in multiple lawsuits involving approximately $50 million in settlements or verdicts to date.
- Manages and structures copyright licensing, publishing transactions and copyright disputes for Estate of pre-eminent author and editorial cartoonist.
- Enforced and licensed "rights of publicity" for the library/foundation of a former United States President.
- Represents leading nanotechnology inventors/founders in a variety of technology transfer and emerging company transactions.

Publications

- "Navigating Entrepreneurship and Ethics in Law and Business," *The Federal Lawyer*, August 2001.

ALSTON+BIRD LLP

Paul G. Martino
Alston & Bird LLP
950 F Street, N.W.
Washington, DC 20004-1404
202-756-3439
paul.martino@alston.com

Services
Legislative & Public Policy
Financial Markets Crisis Task Force
Privacy & Security
Global Business Strategies
Technology
Intellectual Property
Telecommunications Policy & Regulation
Intellectual Property
Financial Services & Products
Corporate & Finance

Education
University of California, Berkeley (J.D., 1994)

Georgetown University (A.B., 1990)

Admitted to Practice
California
District of Columbia

Paul G. Martino

Paul Martino is a partner in the Legislative and Public Policy group and is co-leader of the firm's Privacy & Security Task Force. Paul focuses on representing businesses and coalitions before Congress and Executive Branch departments and agencies on issues affecting financial services, e commerce, data privacy, data security, telecommunications and intellectual property.

Since joining the Washington office in 2005 from his position as a majority counsel to the Senate Commerce Committee, Paul has established himself as a leading industry strategist and skillful advocate for clients in the pursuit of balanced federal legislation and public policy on these matters. Paul also regularly appears as an expert speaker at industry forums, such as those hosted by the U.S. Department of Commerce, the U.S. Chamber of Commerce, the Silicon Valley Association of General Counsels, the Investment Company Institute and the Information Technology Association of America.

Within his areas of expertise, Paul has represented clients on a wide range of issues, including: (i) financial markets crisis; (ii) data privacy and security matters, including breach notification compliance; (iii) Internet advertising, spam, spyware, phishing, and other cybercrime and online consumer protection concerns; (iv) telecommunications issues, including behavioral targeting and FISA concerns; and (v) patent, trademark and copyright issues, including brand abuses, domain name issues and digital media content protection.

Paul previously served as a majority counsel to the Senate Commerce Committee where he was a principal advisor on electronic commerce, telecommunications and intellectual property issues to then-Chairman John McCain (R-AZ). During his nearly four years of service, Paul held key roles in the drafting, consideration and passage of significant legislation, including the "Dot Kids Implementation and Efficiency Act of 2002," the "CAN-SPAM Act of 2003," the "ENHANCE-911 Act of 2004," and the "Family Entertainment and Copyright Act of 2004" (FECA). In particular, Paul negotiated important revisions to FECA on behalf of Senator McCain prior to its Senate passage, and also led the negotiations between Senate and House staff that enabled the passage of the CAN-SPAM Act in 2003.

Before working in the Senate, Paul counseled private and public technology companies on corporate and transactional matters in Silicon Valley from 1994 to 2001. Paul was a founding corporate associate of the law firm of Gunderson Dettmer, and he began his legal career as a business and technology associate with Brobeck, Phleger & Harrison. Paul

received his J.D. from the University of California at Berkeley School of Law (Boalt Hall), and his A.B., magna cum laude, in government from Georgetown University, where he was elected to Phi Beta Kappa.

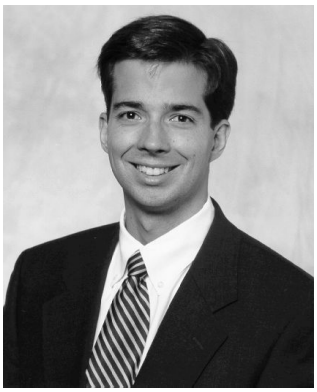
Representative Experience

- Represents clients on the legislative and public policy aspects of the financial markets crisis, including implementation and oversight of the Troubled Asset Relief Program (TARP) by Treasury, initiatives of the Federal Deposit Insurance Corporation (FDIC), and other congressional and federal department and agency efforts to address the financial markets crisis.
- Represents a global telecommunications company on federal legislative issues affecting the telecommunications industry.
- Represents a leading nationwide credit reporting agency and global consumer information services company on a variety of legislative and regulatory issues.
- Represents leading providers of core processing for financial institutions, including electronic payments systems, on a variety of federal legislative and regulatory issues.
- Represents a national association of retail companies on organized retail crime legislation and related consumer protection issues.
- Represents a business coalition of domestic and international brand-name companies that supports federal legislation and other policy initiatives to address persistent and costly online trademark infringement and other abuses of corporate brands and Internet domain names, such as cybersquatting and domain name tasting.
- Represented a national business coalition of companies and industry associations that supports federal legislation to advance the growth of electronic commerce and address privacy concerns.
- Represented an online behavioral marketing firm in federal and state legislative issues addressing online advertising and spyware.
- Represented a global company that secures online payment processes on federal legislation addressing Internet gambling.
- Represented a global transportation and logistics company, a nationwide health services company, and an asset management systems company, among others, in developing comprehensive investigations and response strategies to data security breaches in compliance with all federal and state laws that require notification to affected individuals and to other public and private entities.

Recent Publications

- "Outlook for the 111TH Congress & President-Elect Barack Obama," *Legislative and Public Policy Advisory*, Alston & Bird LLP, November 6, 2008.
- "States Adopting Aggressive New Privacy and Data Security Laws and Regulations," *Privacy and Security Task Force Advisory – Special Update*, Alston & Bird LLP, October 7, 2008.
- "Brief for Executives: Social Security Number and Merchant Liability Legislation," *Legislative & Public Policy Advisory,* Alston & Bird LLP, November 2, 2007.
- "Selected Federal Legislative Developments," *Electronic Banking Law and Commerce Report*, Vol. 12, No. 5, June 2007.
- "Preliminary Legislative & Public Policy Outlook for the 110th Congress (2007-08)," *Legislative & Public Policy Advisory,* Alston & Bird LLP, November 17, 2006.

ALSTON+BIRD LLP



Todd S. McClelland
Alston & Bird LLP
950 F Street, NW
Washington, DC 20004-1404
202-756-3418
todd.mcclelland@alston.com

Services
Energy & Project Finance
Sourcing & Complex Procurement
Intellectual Property
IP & Technology Transactions
Patents
Mechanical Patents
Technology
Energy & Sustainability
CleanTech
Energy, Environmental & Land Development

Education
Florida State University
(J.D., 1998)

Georgia Institute of Technology
(B.ME, 1994)

Admitted to Practice
U.S. Patent and Trademark Office
Georgia
District of Columbia (Pending)

Todd S. McClelland

Todd McClelland specializes in strategic corporate projects that include significant technology, IP, outsourcing, or energy components. His practice scope includes IT systems procurement and infrastructure, outsourcing projects, energy policy, construction projects, intellectual property management, business model innovation activities and technology and energy company representation. In addition to his transactional practice, Todd is a registered patent attorney and provides counsel on patent licensing, avoidance and procurement.

Todd is featured in Chambers USA: *America's Leading Lawyers for Business* for his outsourcing practice. He is the current chair of the Intellectual Property Law Section of the State Bar of Georgia. Todd is a frequent speaker at professional seminars and author of articles on such topics as open source software, digital media convergence, cloud computing, data security and privacy, IP protection strategies, and emerging renewable energy technology issues.

Todd received his J.D. in 1998 from Florida State University where he was a member of the *Florida State University Law Review*, and was the executive editor of Florida State's *Journal of Land Use and Environmental Law*. He received a B.S. in Mechanical Engineering, with high honors, in 1994 from the Georgia Institute of Technology (Georgia Tech) where he focused on controls and power plant systems design. Prior to attending law school, Todd worked as an engineer for Factory Automation Systems in Atlanta, Georgia, where he designed software and hardware automation systems for companies such as Coca-Cola and the Ford Motor Company.

Publications

- "Open Source Basics and a Snapshot of the SCO Litigation," *Electronic Banking Law and Commerce Report*, 2004.
- "Open Source Subject to Challenge," *Charlotte Business Journal*, 2004.

ALSTON+BIRD LLP

David S. Teske
Alston & Bird LLP
One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404-881-7935
david.teske@alston.com

Services
Intellectual Property
IP Transactions
Trademarks & Copyrights
Technology

Education
University at Buffalo
(J.D., 1993)

University at Buffalo
(B.S., 1990)

Admitted to Practice
Georgia
New York
U.S. Patent and Trademark Office

David S. Teske

David leads the firm's IP Technology and Transactions Group, and concentrates his practice on the exploitation, leveraging and transfer of technology and intellectual property rights through complex transfer and licensing transactions. He works with all types of clients, from Fortune 50 corporations to start-up companies. David has counseled his clients in all types of Internet and e-commerce based activities including assisting in the establishment of an Internet-based music, video and media storefront and an Internet-based global shipping and transportation services. He has extensive experience in patent and software licensing with an emphasis on free and open source software; diligence of intellectual property portfolios in the mergers and acquisitions context, including the media and entertainment industry; and counseling clients on the establishment, exploitation and maintenance of their intellectual property portfolios.

David received his J.D. degree in 1993 and B.S. in aerospace engineering in 1990, both from the University at Buffalo, and is also admitted to practice before the United States Patent and Trademark Office. By virtue of his technical background and training, he brings a deep understanding of technologies to his work. During his career, he has prepared and filed patent applications, trademark registration applications and copyright registration applications. He has litigated patent, trademark and copyright infringement actions. He is a frequent speaker on legal issues ranging from digital entertainment to free and open source software before industry groups, fellow attorneys and law school students.

Representative Experience

- Technology transfer licensing agreement between a start-up company having expertise with femtocell technology and a larger consumer electronics company.
- Represented a municipal entity to establish a fiber-optic based Internet-phone-video service for consumers and businesses.

Publications

- "Beware the Patent Troll," *GameDailyBiz*, September 19, 2006.

ALSTON+BIRD LLP

Katherine M. Wallace
Alston & Bird LLP
One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404-881-4706
katherine.wallace@alston.com

Services
Intellectual Property
IP Transactions
Trademarks & Copyrights
Data Privacy & Security
Advertising & Marketing

Education
University of Georgia
(J.D., 2000)

Georgia Institute of Technology
(B.S., 1996)

Admitted to Practice
Georgia

Katherine M. Wallace

Katherine Wallace focuses her practice on all aspects of intellectual property transactional matters, with a particular emphasis on advertising, marketing and sponsorship matters as well as a wide range of licensing and technology transactions. This includes general advice on the protection and enforcement of intellectual property, including counseling on licensing strategies for use, integration and ownership of licensed technology in products for commercial distribution, trademark enforcement and brand protection, e-commerce transactions and strategic alliances.

As a member of the firm's Advertising and Marketing Group and electronic entertainment task force, Katherine's practice includes counseling in the areas of sports and entertainment properties, electronic entertainment and video game development and licensing, content licensing and publishing. Katherine has experience drafting and negotiating a diverse range of agreements in a variety of industries, including, license agreements, sponsorship agreements, master advertising agreements, consulting agreements, technology services agreements, web site development and fulfillment agreements, publishing agreements, retail license and distribution agreements, and co-branding and cross-marketing agreements. Her practice also involves counseling on a variety of complex promotional activities, including giveaways, contests, sweepstakes promotions, direct-to-consumer advertising and telemarketing campaigns.

Katherine received her undergraduate degree, with highest honors, from the Georgia Institute of Technology in 1996. Katherine received her J.D., magna cum laude, in 2000 from The University of Georgia School of Law, where she was an articles editor for the *Georgia Law Review*.

Representative Experience

- Counsel to major entertainment company regarding licensing and distribution of video game content for online service and development of massively multiplayer online game.
- Regularly advises clients in various industries regarding integrated marketing and promotional campaigns, including administration of complex games of chance promotions in all forms of media.
- Counsel to major sports property regarding international trademark protection and enforcement.

ALSTON+BIRD LLP

Michael Zweiback
Alston & Bird LLP
333 South Hope Street
16th Floor
Los Angeles, CA 90071
213-576-1163
michael.zweiback@alston.com

Services
Litigation
Commercial Litigation
IP Litigation
Investigations - Government & Special
Data Privacy & Security
Government Contracts
Health Care

Education
Loyola Law School Los Angeles
(J.D., 1989)

University of California, Los Angeles
(B.A., 1986)

Admitted to Practice
California

Michael Zweiback

Michael Zweiback is a partner in the firm's Los Angeles office focusing his practice on governmental and corporate investigations, white collar criminal defense, environmental crimes, privacy and data security matters. He joins the firm from the U.S. Attorney's Office in Los Angeles, where he had been chief of the Cyber and Intellectual Property Crimes Section since 2007.

In 1990, Michael began his service in the U.S. Attorney's Office, where his practice included the investigation and prosecution of intellectual property offenses, complex business crimes, white-collar fraud including health care fraud and corruption matters. During this time, Michael successfully prosecuted over 20 complex federal jury trials. In addition, Michael served for two years as deputy chief of the Organized Crime Strike Force and three years as the deputy chief of the Organized Crime and Terrorism Section, supervising over 15 prosecutors and staff members.

In 2005, Michael joined the agency's Cyber & Intellectual Property Crimes Section. He was promoted to chief two years later. As chief, his responsibilities included the investigation and prosecution of complex computer crimes involving the intrusion of corporate and government computer networks and e-commerce fraud schemes. He also prosecuted offenses involving the theft of intellectual property, including the theft of corporate trade secrets, criminal copyright, trademark, and violations of the Digital Millennium Copyright Act. His supervisory responsibilities included the review of charging decisions and the supervision of investigations and trials.

While with the U.S. Attorney's office, Michael was the recipient of the Director's Award for Superior Performance as an Assistant U.S. Attorney in 1997 and 1999. He was also awarded the Department of Justice Special Achievement Award in 1993 and 1996 and was an instructor for the Attorney General's Advocacy Institute.

Michael received his J.D. from Loyola Law School in 1989 and his B.A. from the University of California, Los Angeles in 1986.

Representative Experience

During his tenure, Michael was primarily responsible for several high-profile investigations and prosecutions, including:

- Successfully prosecuted the largest domestic seizure of counterfeit business software and licenses (*United States v. Sanh Thai, et. al.)*.

- Operation Summer Solstice, largest international seizure of counterfeit software. First coordination of law enforcement efforts in intellectual property matters between the United States and China.
- Investigation and prosecution of a computer intrusion into the University of Southern California on-line student application database resulting in the theft of student applicant social security numbers (*United States v. Eric McCarty)*.
- Investigation and prosecution of a civilian scientist for the theft of classified national security information from a defense contractor (*United States v. Abraham Lesnick)*.

STROZ FRIEDBERG

JAMES M. AQUILINA

EXECUTIVE MANAGING DIRECTOR AND DEPUTY GENERAL COUNSEL

1925 Century Park East
Suite 1350
Los Angeles, CA 90067
Tel: 310.623.3301
Fax: 310.623.3277
jaquilina@strozllc.com

As Executive Managing Director and Deputy General Counsel, James M. Aquilina contributes to the management of Stroz Friedberg and the handling of its legal affairs, in addition to having overall responsibility for the Los Angeles and San Francisco offices. He supervises numerous digital forensic and electronic discovery assignments for government agencies, major law firms, and corporate management and information systems departments in criminal, civil, regulatory and internal corporate matters, including matters involving e-forgery, wiping, mass deletion and other forms of spoliation, leaks of confidential information, computer-enabled theft of trade secrets, and illegal electronic surveillance. He has served as a neutral expert and has supervised the court-appointed forensic examination of digital evidence. Mr. Aquilina also has led the development of the firm's online fraud and abuse practice, regularly consulting on the technical and strategic aspects of initiatives to protect computer networks from spyware and other invasive software, malware and malicious code, online fraud, and other forms of illicit Internet activity. His deep knowledge of botnets, distributed denial of service attacks, and other automated cyber-intrusions enables him to provide companies with advice and solutions to tackle incidents of computer fraud and abuse and bolster their infrastructure protection.

Prior to joining Stroz Friedberg, Mr. Aquilina was an Assistant U.S. Attorney ("AUSA") in the Criminal Division of the U.S. Attorney's Office for the Central District of California, where he most recently served as a Computer and Telecommunications Coordinator (one of the lead computer crimes prosecutors) in the Cyber and Intellectual Property Crimes Section. He also served as a member of the Los Angeles Electronic Crimes Task Force and as chair of the Computer Intrusion Working Group, an inter-agency cyber-crime response organization. As an AUSA, Mr. Aquilina conducted and supervised investigations and prosecutions of computer intrusions, extortionate denial of service attacks, computer and Internet fraud, criminal copyright infringement, theft of trade secrets, and other abuses involving the theft and use of personal identity. Among his notable cyber cases, Mr. Aquilina brought the first U.S. prosecution of malicious botnet activity for profit against a prolific member of the "botmaster underground" who sold his armies of infected computers for the purpose of launching attacks and spamming, and used his botnets to generate income from the surreptitious installation of adware; tried to jury conviction the first criminal copyright infringement case involving the use of digital camcording equipment; supervised the government's continuing prosecution of Operation Cyberslam, an international intrusion investigation involving the use of hired hackers to launch computer attacks against online business competitors; and oversaw the collection and analysis of electronic evidence relating to the prosecution of a local terrorist cell operating in Los Angeles.

During his tenure at the U.S. Attorney's Office, Mr. Aquilina also served in the Major Frauds and Terrorism/Organized Crime Sections where he investigated and tried numerous complex cases, including a major corruption trial against an IRS Revenue Officer and public accountants; a fraud prosecution against

1925 Century Park East
Suite 1350
Los Angeles, CA 90067
Tel: 310.623.3301
Fax: 310.623.3277
jaquilina@strozllc.com

JAMES M. AQUILINA

EXECUTIVE MANAGING DIRECTOR AND DEPUTY GENERAL COUNSEL

the French bank Credit Lyonnais in connection with the rehabilitation and liquidation of the now defunct insurer Executive Life; and an extortion and kidnapping trial against an Armenian organized crime ring. In the wake of the September 11, 2001 attacks, Mr. Aquilina helped establish and run the Legal Section of the FBI's Emergency Operations Center.

Before public service, Mr. Aquilina was an associate at the law firm Richards, Spears, Kibbe & Orbe in New York, where he focused on white collar defense work in federal and state criminal and regulatory matters.

Mr. Aquilina served as a law clerk to the Honorable Irma E. Gonzalez, U.S. District Judge, Southern District of California. He received his B.A. *magna cum laude* from Georgetown University, and his J.D. from the University of California, Berkeley School of Law, where he was a Richard Erskine Academic Fellow and served as an Articles Editor and Executive Committee Member of the *California Law Review.*

He serves as an Honorary Council Member on cyber-law issues for the International Council of E-Commerce Consultants ("EC-Council"), the organization that provides the CEH (Certified Ethical Hacker) and CHFI (Certified Hacking Forensic Investigator) certifications to leading security industry professionals worldwide.

Mr. Aquilina is the co-author of *Malware Forensics: Investigating and Analyzing Malicious Code,* a book recently published by Syngress Publishing, Elsevier Science & Technology Books, which details the complete process of responding to the malicious code incidents victimizing private and public networks worldwide.

Tom Arbogast

Vice President and Director of Commercial Collaboration, BT Design

Tom is Vice President and Director of Commercial Collaboration for BT Design, BT's IT arm, comprised of nearly 20,000 global employees. He handles major IT supplier, customer and outsourcing negotiations and oversees the implementation of large IT projects from a commercial perspective. Prior to joining BT, he served as an Executive Vice President for a small telco and also worked in a business development/commercial-legal capacity for a large professional services consulting company. He previously worked as appellate counsel in Canada and has argued numerous cases before the Supreme Court of Canada and the BC Court of Appeal.

Mark M. Ishikawa

Chief Executive Officer, BayTSP

Mr. Ishikawa is an expert in the fields of Internet content distribution, spidering, electronic security, networking and database design and has served in a variety of executive level positions in numerous Silicon Valley technology companies. Over the course of his 25 years in the computer services industry, Mr. Ishikawa has engineered and managed large scale databases, wide-area networks, branding, and encryption systems for organizations ranging from the U.S. Department of Defense to Hewlett Packard. Prior to founding BayTSP in 1999, he served as Chief Operating Officer of Infonent.com, Inc.