Cyberspace LAWYER

August 2009 ■ Volume 14 ■ Number 7

Recent Trends in Domain Name Registrations and Cybersquatting

BY ALEXANDRE MONTAGU & THOMAS WALSH

Alexandre Montagu (alex@montagulaw.com) is a founding Partner of Montagu Law, P.C., New York City (http://www.montagulaw.com). Thomas Walsh (tom@montaguelaw.com) is an associate with the firm.

Introduction

The passage of the Anticybersquatting Consumer Protection Act (the "ACPA") was heralded as a major weapon to combat cybersquatting. Yet, nine years later, cybersquatters are more prevalent than ever. In 2007, a record 2,156 complaints alleging cybersquatting were filed with WIPO.

In an increasingly digitized world, a company's top level domain name may be more valuable than its physical address, a fact that has not escaped cybersquatters, who have become more prevalent than ever. In order to be prepared to offer competent advice in this area, practitioners must stay abreast of current practices by cybersquatters, as well as potential responses thereto.

This article will discuss some recent trends in the area of domain name registration practices, as well as the long-standing problem of cybersquatting related to new product names or company names following a merger.

Domain Name Tasting

After registering a domain through an ICANN-accredited registrar, there is a 5-day grace period within which a full refund can be obtained if the registrant elects not to keep the domain. *Domain name tasting* is the practice of registering domains (often in bulk) for the purpose of using the 5-day grace period to determine whether sufficient pay-per-click revenue will be earned to offset the cost of registering a particular domain. The registrant will then drop any domains that do not provide sufficient revenue and obtain a full refund. It is likely that many of the "successful" domains incorporate the trademarks of others in some way, either through misspellings or in combination with other terms. This practice has become very com-

CONTINUED ON PAGE 4

Content HIGHLIGHTS

Complete Table of Contents listed on page 2.

WEST®

40731749

Table of CONTENTS

Cyberspace Lawyer
West Legalworks
195 Broadway, 9th Floor
New York, NY 10007

One Year Subscription ■ 11 Issues ■ $451.00
(ISSN#: 1088-0593)

Please address all editorial, subscription, and other correspondence to the publishers at west.legalworksregistration@thomsonreuters.com

From the EDITOR

Be Careful What You Wish For

Last year, a single mother from Duluth, Minnesota was found to have infringed the copyrights on 24 songs by making them available in a shared folder on her computer, and a jury awarded the record companies $223,000, or $9250 per song. However, after the verdict was rendered, the judge, on his own motion, set the verdict aside because of an error in one of the jury instructions. That gave the defendant, Jammie Thomas, a second chance. According to news reports, she rejected efforts by the RIAA to settle the case for $25,000 or so, opting for a new trial.

The second trial recently ended, with the jury awarding the record companies a whopping $1.92 million in damage, or $80,000 per song. *Be careful what you wish for.*

Even the record companies' lawyers were shocked at the size of the verdict. Yet, one would think the record companies would be ecstatic. If the purpose of the lawsuits against filesharers was to deter such activities, one would think that they would have thought the result beyond their wildest dreams.

But there is a potential dark cloud hanging over this verdict. The extraordinarily large award provides an opportunity for the defendant to argue that the award is denial of due process under several recent U.S. Supreme Court cases that have taken aim at excessive punitive damages. The Supreme Court has focused on the ratio between the actual damages suffered by the plaintiff and the punitive damages awarded. In the *Thomas* case, the defendant has argued that because the individual songs are available on iTunes for $1.29 or less, the ratio of the record companies' actual damages ($1.29 x 24) and the statutory damages per song is 1:62,015. Even if you look at the cost of a complete CD containing the 24 songs at approximately $15 per CD, the ratio is still a whopping 1:5,333.

In papers filed after the verdict was entered, the defendant assert:

> **Although the Supreme Court has declined to state a bright-line rule about the maximum permissible ratio, it has repeatedly held that "few awards exceeding a single-digit ratio between punitive and compensatory damages, to a significant degree, will satisfy due process."**

It is unclear whether the Supreme Court would consider damages set by statute, as is the case with this verdict, to be equivalent to punitive damages. But since the jury is allowed to set the amount, up to $150,000 per song, a strong argument can be made that the unbridled discretion of a jury to award statutory damages that may be in a ratio of 1:100,000 or more are "punitive" in nature, particularly in a situation such as this one, where the defendant's actions were non-commercial.

So by pushing for a large award of statutory damages, the record companies may end up having the entire statutory damages scheme held unconstitutional. *Be careful what you wish for.*

MICHAEL D. SCOTT

EDITOR-IN-CHIEF

BLOG: WWW.SINGULARITYLAW.COM

CONTINUED FROM PAGE 1

mon. The CEO of GoDaddy.com noted that "In February 2007, 55.1 million domain names were registered. Of those, 51.5 million were canceled and refunded just before the 5 day grace period expired and only 3.6 million domain names were actually kept."[1]

In January 2008, ICANN proposed several possible solutions; however, it could take years for any changes to be agreed upon and implemented. In the meantime, at least one company has attempted to combat this practice in court – Verizon commenced litigation in Federal District Court of the Central District of California against a company that had both tasted and registered a large number of domains that allegedly incorporated Verizon's trademarks, as well as the company's registrar (which is affiliated with the company). Verizon contended that the registration of these domain names violated the ACPA. On June 30, 2008, the Court rejected the defendants' argument that they were merely reserving the domains during the tasting period as opposed to registering them, and found that the defendants' conduct constituted bad faith intent to profit under the ACPA.[2] The Court also issued a preliminary injunction against the defendants prohibiting them from registering any domain names that are confusingly similar to Verizon's marks.

This decision is important, as it is believed to be the first decision which has found liability for domain tasting, as well as the first time that a registrar has lost an ACPA lawsuit. Soon after this decision was issued, the parties reached a settlement whereby the defendants agreed to be permanently enjoined from registering any domain names that are confusingly similar to Verizon's marks.

Front-Running

Front-running occurs when a domain name registrar (or a registrar insider) uses insider information to register domains that generate numerous lookup requests in an effort to either re-sell them or earn advertising revenue. This practice recently gained attention when Network Solutions was accused of front-running in connection with its policy of automatically reserving a domain name every time someone conducted a search for a domain on Network Solution's website, and holding it for the 5-day grace period. The practical effect of Network Solution's practice was that anyone who searched for a domain on Network Solution's website and then attempted to register it through another registrar (many of whom offer cheaper prices than Network Solutions), would be prevented from doing so. In February 2008, a class action lawsuit was filed against Network Solutions in connection with the front-running allegations under the following theories: fraudulent concealment; aiding and abetting fraudulent concealment; and unjust enrichment. The lawsuit is currently pending.

Despite the long-standing suspicions by many people concerning the existence of front-running, an ICANN panel recently investigated 120 cases of alleged front-running and found that there was insufficient evidence that such practices exist in any appreciable measure[3]. Nevertheless, it is a topic that is sure to remain in the minds of many in the domain name industry, and companies should be cognizant of registrars' policies in this area prior to performing any availability searches on the respective websites.

Use of Privacy Services

Another vexing issue confronting trademark owners who seek to recover unauthorized domains is cybersquatters' use of privacy or proxy registration services. These services allow registrants to conceal their identity on the publicly available Whois records. This can potentially hinder trademark owners in various ways. First, it hinders the initial investigation into potentially infringing activity connected to unauthorized domain registrations. Second, it impairs communication with the registrant.

The first step in recovering a domain is usually to send the registrant a cease and desist letter. However, because the only publicly available address for the registrant is the privacy service address listed in the Whois record, the trademark owner cannot ascertain whether or not the notice was received. These services provide potential cybersquatters with a virtual carte-blanche to register infringing domains. Potential cybersquat-

ters know that, as opposed to litigation, it will be more cost efficient for a company to seek recovery of an infringing domain through the UDRP process. And at that point, the registrant can simply choose not to respond. Consequently, the only harm suffered by the registrant will be the loss of the domain. Therefore, if a particular company is a common victim of cybersquatters, it may elect to file a federal a lawsuit under the ACPA because damages are available under the ACPA and a favorable decision could also have a deterrent effect on future cybersquatters.

Domain Name Warehousing

Domain name warehousing refers to the practice by registrars of obtaining control of domains after they expire and either auctioning them off or using them to generate advertising revenue. It was recently reported that GoDaddy had been warehousing domains by transferring ownership of some expired domains to one of its subsidiaries.[4] GoDaddy had taken steps to hide this practice, such as incorporating the subsidiary in a different state and using a Whois privacy service when transferring the domains.

However, the subsidiary's connection to GoDaddy was revealed in a 2006 IPO. In response to the recent publicity surrounding their warehousing practices, GoDaddy's CEO indicated that they are shutting down the subsidiary and placing all of its domains up for auction.[5] It appears that sometimes public shame may be the most effective way to combat unscrupulous domain name registration practices.

Cybersquatting Related to Mergers/ New Product Names

In situations such as mergers or new product launches, if companies are not careful, one simple oversight can cost them hundreds of thousands of dollars. It cannot be overstated that practitioners and their clients should be proactive and vigilant in connection with domain name registrations before a product is launched or prior to a merger being announced.

However, it is also important to recognize that there are certain instances where proactively registering such domains is not a viable option. For example, if a company is contemplating a merger, it will likely want to avoid leaking that information to the public. MCI WorldCom encountered this very situation in the days leading up to its merger with SkyTel Communications in 1999. After the domain name registration became public, SkyTel's stock rose 16 percent. MCI then denied that the domain name registration was an indication of the company's intention, and the share price dropped, only to rise again after MCI announced the acquisition a few days later. MCI was later sued for allegedly influencing the price of the stock.

Adding support to this notion is a recent study conducted by London's Cass Business School, which found that fewer than half of merger and acquisition transactions are completed if they are prematurely leaked, compared to a 72% completion rate for deals that are not leaked.[6] Consequently, under merger or new product launch scenarios, companies should be proactive with their domain registrations, but cognizant of the way in which the domains are registered and the unintended consequences that could arise as a result thereof.

Recovery of Infringing Domains

There are a few ways in which those victimized by cybersquatters can attempt to recover their domains. The UDRP process is the fastest and most cost-efficient manner in which to recover such domains. In order to prevail, a complainant must demonstrate (i) that the domain name is identical or confusingly similar to a trademark in which the complainant has rights; (ii) that the registrant has no rights or legitimate interest in the domain; and (iii) that the domain name was registered and used in bad faith. In most cases, if the cybersquatter does not mount a defense, it will only take about a month-and-a-half to receive a decision after filing a complaint. And the vast majority of UDRP decisions are reached in favor of the complainant. However, there are some instances where the UDRP process may not be sufficient.

One example where the UDRP process may not suffice is when a UDRP decision has been challenged by the registrant. According to ICANN Rules, a UDRP decision will be stayed if the losing party initiates an action challenging the decision in a court of competent jurisdiction within ten days after the decision is reached. This can be especially burdensome for the complainant when the registrant initiates a court proceeding in another country. In this situation, the complainant may elect to bring an *in rem* proceeding in a U.S. Federal Court in the district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located.[7] This option is only available, however, if the Court lacks personal jurisdiction over the registrant.

In addition to allowing for jurisdiction over a domain name that was registered by someone outside the United States, another benefit of the *in rem* approach is that a foreign cybersquatter may choose not to appear in a court in the United States. If this is the case, it should be relatively easy to obtain a default judgment within a short time period. It is also helpful to know that the Eastern District of Virginia may consider an *in rem* action even if the registrant has already initiated an action concerning the domain in a foreign country.[8]

One drawback to the *in rem* approach is that it does not allow for the recovery of damages. A traditional claim under the ACPA on the other hand allows for damages as high as $100,000 per infringing domain. For instance, Verizon recently obtained a judgment against a cybersquatter in the amount of $33 million ($50,000 per domain).[9] While it may be unlikely that Verizon will ever actually collect the money, the judgment may at least have a deterrent effect on other cybersquatters. In light of the above, it is clear that victims of cybersquatting must be cognizant of the available options and be able to balance various factors before deciding an appropriate response.

1. *See* http://www.bobparsons.me/Whyyoucantgetthedomainnameyouwant GoDaddyrescuesRegisterflycustomers.html.
2. *See* Verizon California, Inc. v. Navigation Catalyst Systems, Inc., 2008 WL 2651163 (C.D. Cal. June 30, 2008).
3. See http://www.icann.org/en/committees/security/sac022.pdf
4. *See* Robin Wauters, "GoDaddy Uses Standard Tactics To Warehouse Domains," Wash. Post, Dec. 3, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/12/04/AR2008120400170.html
5. *See* "Go Daddy To Shut Down Standard Tactics, LLC," *available at* http://domainnamewire.com/2008/12/17/go-daddy-to-shut-down-standard-tactics-llc/
6. *See* http://www.intralinks.com/solutions/ma/information-leaks/information-leaks.pdf
7. This will often be the U.S. Federal District Court for the Eastern District of Virginia, which possesses jurisdiction under the ACPA by virtue of the fact that the registry of all ".com" domain names, VeriSign, is located within its district.
8. *See* NBC Universal, Inc. v. NBCUNIVERSAL.COM, 378 F.Supp.2d 715 (E.D. Va. 2005).
9. *See* Verizon California Inc. v. OnlineNIC Inc., 2008 WL 5352022 (N.D. Cal. Dec. 19, 2008).

Russia Revises the Rules Applicable to State Registration of License

Agreements and Other Forms of Disposal of Rights in Intellectual Property

BY EUGENE ARIEVICH, MARGARITA DIVINA & MARINA SHARAEVA

Eugene Arievich (eugene.arievich@bakernet.com) is a partner, and Margarita Divina (margarita.divina@bakernet.com) and Marina Sharaeva (marina.sharaeva@bakernet.com) are associates in Baker & McKenzie's Moscow office.

Introduction

The act – Order No. 321 of the Ministry of Education and Science of the Russian Federation "On the Approval of the Administrative Regulations to Govern the Performance by the Federal Service for Intellectual Property, Patents and Trademarks of Its Functions to State-Register Agreements on Disposal of Rights to Inventions, Utility Models, Industrial Designs, Trademarks, Service Marks, Protected Computer Programs, Databases, and Integrated Circuit Layouts, as well as Franchising Agreements for Intellectual Property Assets Protected in Accordance with the Patent Legislation of the Russian Federation," dated October 29, 2008 (the "Regulations") – was officially published on June 1, 2009 and came into force on June 12, 2009.

The Regulations supersede the Russian Agency for Patents and Trademark's Orders Nos. 64 of April 29, 2003 and 163 of December 11, 2003, which used to regulate the registration of such agreements (the "Previous Rules"), and establish new rules for the Russian Federal Service for Intellectual Property, Patents and Trademarks ("Rospatent") to act as the registrar in their respect.

Subject to Registration Under the Regulations

The following are subject to registration under the Regulations:

- agreements on assignment of exclusive rights to the following registered intellectual property:
  a) inventions,
  b) utility models,
  c) industrial designs,
  d) trademarks,
  e) integrated circuit layouts,
  f) computer programs, and
  g) databases;
- pledge contracts and subsequent pledge contracts for exclusive rights to registered intellectual property listed in points (a)-(e);
- license agreements and sublicense agreements;
- franchising agreements and sub-franchising agreements;
- amendments to any of the substantial conditions of a registered agreement (an "Agreement"), and the termination of an Agreement;
- mandatory licenses and their termination;
- open licenses and petitions retracting applications for open licenses; and
- transfers of executive rights to registered intellectual property listed in points (a)-(g), and appellations of origin other than on the basis of an Agreement.

Unlike the Previous Rules, the new ones expressly authorize any party to an Agreement to apply for its registration.

New Requirements for Execution of Documents

The Regulations introduce some fundamentally new requirements for the execution of documents.

The corporate names of legal entities, and the first names, middle names or patronymics, and surnames of individuals must now appear in full, without any abbreviations, while the corporate names and addresses of foreign persons must be transliterated and indicated in Cyrillic.

Any registration application must be entirely in the Russian language. Names and legal addresses, whether those of legal entities or those of individuals, may also be indicated in another language for the purposes of the respective publications in Rospatent's official newsletters. A registration application must include a contact mailing address in the Russian Federation.

The new requirements concerning the applicant's identity in the application are as follows:

- its name (if a legal entity) must be identical to that as given in its constituent documents;
- if the applicant is a Russian legal entity, the application must provide its principal state registration number, and if the applicant is a Russian individual entrepreneur, the application must give the principal state number of the entry on the latter's state registration in such capacity; and
- the application of a foreign person must feature the code of the latter's country.

The Regulations also expressly stipulate for the first time that the document verifying payment of the applicable fee is a copy of the corresponding payment order with notation marked by the bank to confirm the payment is made, or a bank receipt confirming receipt of the appropriate payment in cash or by bank transfer from a personal account. The document confirming payment of the fee must refer to a single application, feature at least one patent number or certificate number, and specify the procedure for which the fee has been paid.

The period for checking if a filing meets the applicable registration requirements, i.e., for a validity check, is the same two months after either the filing date of the respective registration application or the submission day of the last document requested by Rospatent. But the Regulations also provide for a formal document inspection, which was absent from clearance procedures under the Previous Rules, and which amounts to an examination of a submission so as to satisfy Rospatent that the required package of documents is complete and there are no execution flaws tha make any part of a document illegible. Ten business days are reserved for this kind of scrutiny after the documents reach Rospatent.

The Regulations give applicants longer (three months instead of the two before) to reply to a request from Rospatent for additional documents, and makes it possible to further extend this period upon a relevant petition (but by no more than another three months).

Disposal of Exclusive Rights

The form of disposal of exclusive rights is still at all times subject to Rospatent registration -- and on the same conditions as before (the respective intellectual property must be already duly registered, the corresponding documents must conform to the applicable requirements and be filed on time, etc.), as well as the following new conditions:

- the information provided about the owner of the respective rights or about the parties to the corresponding Agreement must be consistent with the data recorded in the relevant registers;
- the assignee or licensee of the exclusive rights to a trademark incorporating an appellation of origin as an non-protectable element must have exclusive rights to (use) such appellation of origin;
- an Agreement executed on a paid basis must include a clause on the amount of the fee or on a procedure for its determination; and
- none of the rights constituting the subject matter of the Agreement may go beyond the scope of rights held by its corresponding party.

Disposal of Trademark Rights

The Regulations also supplement the list of conditions (which were also specified in the Previous Rules) whereby the disposal of exclusive trademark rights may not mislead the consumer in respect of the goods/services or their producer/provider. And the Regulations partially complement the features list specified in the Previous Rules -- under this list, assignment of the exclusive right to a trademark may be regarded as misleading – and accordingly can not be registered – as contrary to Item 2 of Article 1488 of the Civil Code of the Russian Federation.

Under the Regulations, the assignment of the exclusive right to a trademark may be regarded as misleading in respect of goods/services or their producer/provider where a trademark includes:

- A designation representing the state emblem, flag or other state symbol and sign, official state name, emblem, abbreviation or full name of an international and interstate organization, their emblems, flags, other symbols and signs, official countermark, seal of guarantee, hallmark, seal, award or other mark of distinction, or a confusingly similar designation that is included as a non-protectable element on the basis of the corresponding competent authority or its right holder's consent, if the trademark is assigned to a party to which such consent was not granted;
- A designation indicating the place of origin or place of sale of the goods included in the trademark as a non-protectable element, if the trademark is assigned to a party located in another geographical area; or
- A designation that is identical or confusingly similar to an official name or images of especially valuable cultural heritage objects of the peoples of Russia, or world cultural or natural heritage objects, or to images of cultural heritage in collections and funds, if the trademark is assigned to a party to which the consent of the right holder was not granted.

The assignment of the exclusive right to a trademark may be regarded as misleading where such assignment concerns the following:

- A trademark that has been recognized as well known under the established procedure;
- A portion of goods and services that are similar to goods and services in relation to which the right holder [trademark owner] retains the right to the trademark;
- A trademark that is confusingly similar to an industrial design, the right to which belongs to the trademark assignor that retains the right to the industrial design;
- A trademarkthat is confusingly similar to a trademark used in relation to similar goods and services, the rights to which trademark are retained by the original right holder; or
- A trademark reproducing a trade name (or an element thereof), the right to which belongs to the trademark assignor that retains the right to the trade name.

Documents to be Submitted

The Regulations contain explicit lists of documents to be submitted for each type of exclusive right disposal.

An applicant is to submit two original counterparts and one uncertified copy of the respective Agreement or of a relevant extract from the Agreement for filing with Rospatent for registration purposes under the Regulations (rather than three originals of the Agreement under the Previous Rules).

Should Rospatent decide to grant a registration application, it should:

1. assign a registration number to the respective event requested to be registered;
2. make a relevant registration entry in the appropriate register;
3. prepare a registration notice in duplicate for the parties to the Agreement or for the licensor and the person granted use rights under a compulsory license;
4. produce an appendix to the respective patent or certificate (or, should exclusive trademark rights be assigned in respect of a portion of the corresponding goods and/or services, a

new certificate) to reflect the effected registration;

5. affix notation to confirm such registration, including its number and date, on the two submitted counterparts of the Agreement;
6. send the above registration notice and appendix to the patent or certificate or new certificate, as well as the two counterparts of the Agreement, to the mailing address specified in the registration application;
7. report the registration in the official newsletters of Rospatent; and
8. publish a posting about the registration on its official website within one month of the registration date.

Should Rospatent decide to turn down a registration application, it should:

1. send a notice regarding such refusal explaining the reasons behind the decision to the applicant;
2. return the two original counterparts of the Agreement to the applicant; and
3. return the document confirming the payment of the fee (except when it was paid for the registration of an Agreement for an integrated circuit layout, a computer program or a database) to the applicant.

The Regulations also establish periods for the review of complaints filed with Rospatent and procedures for challenging any act and/or omission to act on the part of its officers.

Litigation

BY ZACHARY LEVINE

Zachary Levine currently works for a downtown Long Beach, CA litigation firm. He recently graduated from Southwestern Law School where he was a member of the Moot Court Honors Program and participant in the John Marshall Information Technology and Privacy Law Competition.

New Jersey Blogger Denied Shield Law Protection and Liable for Damages Without Evidence of Actual Harm

Too Much Media, LLC v. Hale, No. MON-L-2736-08 (N.J. Super. Ct., June 30, 2009).

Defendant Hale operates various websites where she offers her services as a life coach. These services take a number of forms, including webcam interactions and a blog. Hale has never been employed by any news agency, nor has she ever been paid for the content of her blogs or websites.

In 2007 Hale launched a campaign against criminal activity in the online adult entertainment industry following a problem she experienced with people exposing themselves during webcam sessions on her website. Part of her campaign was a website called Pornafia where she intended to post information on the alleged criminal activity within the adult entertainment industry. Additionally, she registered for at least 2 porn industry online forums to discuss her point of view.

Too Much Media, LLC, ("TMM"), produces an affiliate management software called NATS. In 2008 major news agencies began reporting that TMM became aware of a security breach, which allowed a hacker to access various adult websites' subscriber lists. Hale made several postings to online forums regarding the breach including allegations of statutory violations on the part of the plaintiff as well as claims of impropriety and improper business dealings. In response to Hale's comments Too Much Media brought this action for defamation.

New Jersey's Shield Law states:

> **[A] person engaged on, engaged in, connected with, or employed by news media for the purpose of gathering, procuring, transmitting, compiling, editing or disseminating news for the general public or on whose behalf news is so gathered, procured, transmitted, compiled, edited or disseminated has a privilege to refuse to disclose, in any legal or quasi-legal proceeding or before any investigative body, including, but not limited to, any court, grand jury, petit jury, administrative agency, the Legislature or legislative committee, or elsewhere.**

To invoke this protection a defendant must establish a connecting with the "news media," the statutory definition of which has been expanded by case law to include such media as magazines, biographical novels, and documentary videotapes. The court was unconvinced that Hale could establish any statutory connection to news media. While the defendant argued that one of the sites she posted her comments on billed itself as the "Wall Street Journal" of porn, that alone did not transform the site into anything more than an online forum. Additionally, the court could not find any similarity between the forum and the statutorily recognized forms of media. While the recognized forms also had online components the court was fearful of extending Shield Law protection to "anyone with an email address, with no connection to any legitimate news publication."

Even though Hale's stated intent for creating her blog was to disseminate "news to the general public," the comments in question were made on a third party site without ever contacting TMM's representatives for their side of the story. There was nothing in Hale's actions or comments that resembled the activities of a member of legitimate media. Because of Hale's status as an individual with no connection to "news media" she was not allowed to avail herself of the Shield Protection law. Because the court did not find membership in adult websites a matter of public concern, the plaintiff also did not have to show actual malice for its claims. Furthermore, as Hale's statements concerned conduct relating to a criminal offense punishable by imprisonment or regarded by the public as regarding moral turpitude, as well as the plaintiff's ability to perform its trade or profession, TMM was not required to show actual harm to bring a claim for damages.

Cybersecurity: A Briefing

BY R. MICHAEL SENKOWSKI & MIMI W. DAWSON

R. Michael Senkowski (msenkowski@wileyrein.com) is a partner and Mimi W. Dawson (mdawson@wileyrein.com) is a Senior Public Policy Consultant in the Washington, D.C. offices of Wilen Rein LLP.

The Obama Administration's Cybersecurity Strategy

On May 29, 2009, the White House released the "Cyberspace Policy Review" (the Review) – often referred to as the Hathaway Report. Melissa Hathaway, acting Senior Director for Cyberspace for the National Security Council, led the Review. The Review was initiated by President Obama in February 2009 in order to do a "comprehensive 'clean-slate' review to assess U.S. policies and structures for cybersecurity." This Review – while light on specifics – sets the stage for high-level attention on all things related to cybersecurity and seeks to promote a comprehensive approach to

securing digital infrastructure. The Review is a key indicator of this Administration's approach to cybersecurity and will prompt continuing discussion of these issues in Congress.

With the release of the Review, the President announced he would appoint a White House cybersecurity policy official to lead cybersecurity-related policymaking and cyber-incident response efforts. This official would report to the National Security Council and the National Economic Council. The President is expected to name the person to fill this position during the week of June 1. Potential candidates for the position include Hathaway; Microsoft Corp. Vice President Scott Charney, who formerly ran the Justice Department's computer-crime unit and Maureen Baginski, who has held senior National Security Council and FBI positions.

The Review addressed missions and activities associated with information and communications infrastructure, including computer network defense and other areas such as information assurance, counterintelligence, counterterrorism, telecommunications policies and general critical infrastructure protection. Key points in the report include the following:

Leading from the Top

- The President should appoint a cybersecurity official with clear presidential support and authority to participate in all appropriate economic, counterterrorism and science and technology policy discussions to inform them of the cybersecurity perspectives.
- The cybersecurity policy official should not have operational responsibility or authority, nor the authority to make policy unilaterally, but using interagency coordination processes, the cybersecurity policy official should harmonize cybersecurity-related policy and technology efforts across the federal government.
- All federal departments and agencies should establish a point-of-contact in their respective executive suites, who is authorized to interface with the White House on cybersecurity-related issues.
- The cybersecurity policy official should prepare for the President's consideration an updated national strategy to secure the information and communications infrastructure.
- The Administration should work with Congress to update the Federal Information Security Management Act of 2002 (FISMA) to hold department and agency officials responsible for cybersecurity and secure systems.

Building Capacity for a Digital Nation

- The federal government, with the participation of all departments and agencies, should expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
- The President's cybersecurity policy official, in coordination with the ICI-IPC, should consider how to better attract cybersecurity expertise and to increase retention of employees with such expertise within the federal service.

Sharing Responsibility for Cybersecurity

- Industry and governments share the responsibility for the security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies.
- Government can facilitate private sector engagement by considering incentive-based legislative or regulatory tools to enhance the value proposition and fostering an environment that facilitates and encourages partnership and information sharing.
- The President's cybersecurity policy official should work with relevant departments and agencies and the private sector to examine existing public-private partnership and information sharing mechanisms to identify or build upon the most effective models.
- Federal government should develop a proactive engagement plan for use with international standards bodies (UN, Group of Eight,

NATO, etc). Agreements, standards or practices promulgated in these organizations have global effects and cannot be ignored. The Review recommends further study on whether and in what ways elements of the information and communication infrastructure ought to be treated as a global commons.

Creating Effective Information-Sharing and Incident Response

- The newly created cybersecurity policy official is the White House action officer for cyber incident response.
- In order to improve situational awareness and response capability the federal government should explore long-term architectures for intrusion detection and prevention systems, leverage long-term investments in the development of cryptologic and information assurance technologies and supporting infrastructure.
- Develop options for cybersecurity-related information sharing – such as trusted third hosts – to enhance information-sharing with the private sector to improve incident response.

Encouraging Innovation

- The federal government should provide a framework for research and development strategies that focus on game-changing technologies that will help meet infrastructure objectives, building on the existing Networking and Information Technology Research and Development (NITRD) strategies and other R&D-related work.
- The federal government—in collaboration with industry and the civil liberties and privacy communities—should build a cybersecurity-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies.
- The emergence of new centers for manufacturing, design and research across the globe raises concerns about the potential for easier subversion of computers and networks through subtle hardware or software manipulations. The best defense may be to ensure U.S. market leadership through continued innovation that enhances U.S. market leadership and the application of best practices in maintaining diverse, resilient supply chains and infrastructures.
- Federal policy must address national security requirements, protection of intellectual property and the availability and continuity of infrastructure, even when it is under attack by sophisticated adversaries. The federal government also must be careful not to create policy and regulation that inhibits innovation or results in inefficiencies or less security.

Action Plans

The Review Team also recommended the following Action Plans:

Cyberspace Policy Review: Near-term Action Plan

- Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
- Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCl activities and, where appropriate, build on its successes.
- Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
- Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
- Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related is-

sues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the federal government.

- Initiate a national public awareness and education campaign to promote cybersecurity.
- Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
- Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement.
- In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Cyberspace Policy Review: Mid-term Action Plan

- Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
- Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
- Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
- Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the federal government.
- Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness and inform incident response capabilities.
- Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning and prioritization of R&D.
- Develop a process between the government and the private sector to assist in preventing, detecting and responding to cyber incidents.
- Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
- Develop solutions for emergency communications capabilities during a time of natural disaster, crisis or conflict while ensuring network neutrality.
- Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
- Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
- Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
- Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable

identity management systems to build trust for online transactions and to enhance privacy.

- Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.

Additional Background on Cybersecurity Strategy in the Executive Branch

During the week of May 26, the Obama Administration also announced that it would combine the Homeland Security Council (HSC) and the National Security Council (NSC) into a new entity called the National Security Staff (NSS). This is important because HSC previously had a significant cybersecurity portfolio. The NSS will comprise approximately 240 staffers who will report to National Security Advisor James L. Jones. This initiative is intended to better coordinate the offices who previously had policy purview over homeland security and national security issues. Both Homeland Security Committee Chairmen Sen. Joe Lieberman (D-CT) and Rep. Bennie Thompson (D-MS) have endorsed this change. Republican reaction to this initiative has been mostly positive, although both Homeland Security Committee Ranking Members Sen. Susan Collins (R-ME) and Rep. Peter King (R-NY) have expressed concerns regarding organizational focus and coordination.

In early 2003, the Bush Administration released the "White House National Strategy to Secure Cyberspace." This strategy document indicated that the Department of Homeland Security (DHS) would play a central role in securing cyberspace and serve as the primary federal point of contact for cyber issues – particularly for the private sector and state and local stakeholders. Late in 2003, Homeland Security Presidential Directive (HSPD)-7 established overall policy for securing critical infrastructure and key resources and identified DHS as a central player in cybersecurity. Specifically, HSPD-7 directed DHS to maintain an organization that serves as focal point for cybersecurity and that facilitates interactions and collaboration between federal agencies and other stakeholders. These documents did not overlook other agencies' core competencies such as the Department of Justice's (DOJ) law enforcement role, Department of Defense's (DOD) national defense role, the CIA's intelligence role, the State Department's international cooperation role and the Department of Commerce's standard setting role (NIST).

Under the previous Administration, the Office of Management and Budget (OMB) also had and is expected to continue to have a significant role in securing federal networks in part because it has oversight for implementation of the FISMA. FISMA requires agencies to inventory and implement security controls for federal information technology systems. However, many experts believe FISMA is inadequate to address federal network cybersecurity issues as it is mainly a reporting mechanism. In 2007, OMB took action to secure federal networks with its mandate for a Federal Desktop Core Configuration (requiring standard security settings for desktops) and the Trusted Internet Connections Program (requiring efforts to minimize federal external connections and to monitor for intrusions).

In January 2008, the Bush Administration launched a classified cyber effort called the Comprehensive National Cybersecurity Initiative (CNCI) that was outlined in Homeland Security Presidential Directive (HSPD-23). CNCI was launched as multi-year $17 billion program, but few details have been released. However, media reports in late 2008 reported senior Administration officials saying that the 12 CNCI objectives are:

- Move towards managing a single federal enterprise network;
- Deploy intrinsic detection systems;
- Develop and deploy intrusion prevention tools;
- Review and potentially redirect research and funding;
- Connect current government cyber operations centers;

- Develop a government-wide cyber intelligence plan;
- Increase the security of classified networks;
- Expand cyber education;
- Define enduring deterrent technologies and programs;
- Develop multi-pronged approaches to supply chain risk management; and
- Define the role of cybersecurity in private sector domains.

As part of the CNCI effort and the continuing TIC effort, the Bush Administration – in 2008 – spent significant time and resources launching an intrusion detection tool called EINSTEIN. This tool was developed by DHS to monitor and automatically collect and analyze information on agency network security. In addition, the National Cybersecurity Center was established within DHS as part of the CNCI to provide situational awareness on network security across the federal government. The CNCI was intended to serve as a cross-domain awareness platform with at least six different agencies with cyber-related responsibilities providing information to CNCI.

Agency Stakeholders in Cybersecurity

Currently–in terms of organization–the Pentagon and the National Security Agency (NSA) safeguard military networks while DHS is responsible for securing the federal civilian networks and for providing assistance largely through information-sharing to the private sector.

Organizationally, DHS has located the cybersecurity portfolio in the National Protection and Programs Directorate (NPPD), which oversees the National Cybersecurity Division and the U.S. Computer Emergency Response Team (US CERT). US CERT is a key operational entity that monitors networks/cybersecurity trends and facilitates information sharing with the private sector. DHS also houses the National Cybersecurity Center.

NPPD also oversees critical infrastructure protection activities – which includes cybersecurity and coordination with the private sector. DHS's infrastructure protection division coordinates the Critical Infrastructure Partnership Advisory Council (CIPAC) – which through a series of cross-sector groups and specific sector groups – facilitates planning and information-sharing between the federal government and the private sector. In 2008, CIPAC established a cross-sector cybersecurity working group to facilitate coordination on cross-sector cybersecurity issues.

Other agencies with cybersecurity responsibilities include: DOJ/FBI, Office of Director of National Intelligence (DNI), DOD, NSA, Department of State and Department of Commerce. The DOJ/FBI bring the law enforcement expertise to bear on cybersecurity issues. DNI has the counterintelligence role while NSA is traditionally the owner of the most robust technology within the federal government for cybersecurity. NSA has been developing tools to monitor federal networks.

In late April 2009, the DOD focused its cybersecurity efforts by establishing a new cyber command that will be led by National Security Agency Director Keith Alexander. Initially, this new command will be part of the U.S. Strategic Command and responsible for securing the military networks and initiating cyber attacks. The new cyber command is expected to be operational in October 2009. DOD has also requested significant funding in its FY 2010 budget to hire hundreds of cybersecurity experts. The State Department will continue its international coordination role while the Department of Commerce's NIST – will likely play a key role setting standards.

Cybersecurity Legislation in the 111th Congress

At the end of this article is a link to a chart entitled "Cybersecurity Legislation in the 111th Congress," which lists pending cyber-related legislation, demonstrates that Congress is focused on cybersecurity this year and is certain to weigh in on a number of cybersecurity issues. The bills by Senate Commerce Committee Chairman Jay Rockefeller (D-WV) (S.773 and S. 778) and Sen.

Tom Carper (D-DE) (S.921) address structural change within the government.

Sen. Rockefeller's bills are the most promising legislative vehicles for enacting cybersecurity structural change this Congress. This legislation like the just released Review would establish a "Cyber Czar." In an effort to combat jurisdictional turf battles, Sen. Rockefeller introduced his proposal into two separate bills. S. 778 creates a new "Cyber Czar" within EOP and has been referred to the Senate Committee on Homeland Security and Government Reform. Meanwhile, the Cybersecurity Act of 2009 (S.773), would create a Cybersecurity Advisory Panel that would advise the President and be composed of outside experts from industry, academia, and nonprofit groups. The bill would also create a public-private clearinghouse for cyber threat and vulnerability information sharing, and establish measurable and auditable cybersecurity standards in coordination with the National Institute of Standards and Technology (NIST). Furthermore, S. 773 creates a number of new Department of Commerce-related action items under the purview of the Cyber Czar. The Administration reportedly provided support and assistance in drafting these bills and it is worth noting that Rockefeller and Snowe have both been very vocal regarding the importance of passing these initiatives.

The United States Information and Communications Enhancement (U.S. ICE) Act of 2009 (S. 921), as introduced by Sen. Carper, would establish a National Office for Cyberspace in the White House, which would oversee the execution of cybersecurity policies and procedures in federal government. The Office's Senate-confirmed director would be charged with working with industry and developing "lock down" configurations for off-the-shelf products and services used by agencies as well as pre-certifying technologies to the extent practicable. In addition, within 180 days of the bill's enactment, Congress would receive a report describing potential cost savings and security enhancements as well as recommendations for legislative or executive branch actions. Individual agencies would have a range of new security responsibilities, including an annual independent evaluation of their information security programs and practices.

Meanwhile, on the House side, Chairman of the House Homeland Security Committee Bennie Thompson has publicly stated that he believes cybersecurity should be controlled by a government agency (DHS) that interfaces with but is not controlled by the NSA or an office within the EOP. Under this proposal, the Homeland Committee will retain jurisdiction and it will address the strong reticence to place the NSA in a leading role due to perceived civil liberties issues. Senate Homeland Security Committee Ranking Member Susan Collins concurred by saying that putting the cybersecurity program in the White House would lead to "more secrecy and less Congressional oversight."

There are also other legislative vehicles related to cybersecurity that are receiving Congressional attention. TheNetworking and Information Technology Research and Development Act of 2009 (H.R. 2020), which was authored by Rep. Bart Gordon (D-TN), has passed the House and now awaits consideration in the Senate. The IT Investment Oversight and Waste Prevention Act (S. 920), introduced by Sen. Tom Carper, was marked up and reported favorably from the Senate Homeland Security and Government Affairs Committee last week. In addition, Rep. Bobby Rush's (D-IL) Data Accountability and Trust Act (H.R. 2221) and Rep. Mary Bono-Mack's (R-CA) Informed P2P User Act (H.R. 1319) have been the focus of recent hearings before the House Energy and Commerce Committee.

Link to chart: http://www.wileyrein.com/docs/docs/278.pdf.

Eric's Blog

ERIC GOLDMAN

Eric Goldman is Assistant Professor and Academic Director of the High Tech Law Institute, Santa Clara University School of Law. He can be reached at egoldman@gmail.com.

Web Developer Didn't "Convert" Website

Citation: *Conwell v. Gray Loon Outdoor Marketing Group, Inc.*, 82S04-0806-CV-00309 (Ind. Sup. Ct. May 19, 2009).

This is a classic cautionary tale about interactions between a web developer/host and a customer. The customer retained the web developer to develop a website. The paperwork between the parties was not a model of clarity. Later, the customer orally asked the developer to modify the site; this time, there is only garbled conversations and no paperwork. The developer modified the site but the customer changed its mind and asked the developer to roll back to the earlier version. But the developer could not do so because it didn't keep a copy of the earlier version (what???). The customer stiffed the developer and the developer took the website offline. The developer sued for non-payment; the customer cross-sued for conversion on the theory that it had paid for the site and had been deprived of its property.

The Indiana Supreme Court wrestles with several questions, concluding that:

1) The relationship was governed by common law principles applicable to services, not the UCC Article 2 applicable to goods. This is a tricky area of the law, but I think this may be the more logical result for a combination web developer/host, especially one who never actually delivers any code to the customer.

2) Was there an enforceable agreement to amend? The trial court said yes, and the Supreme Court saw no reason to override that factual finding.

3) Did the developer convert the code/website by erasing the old version? The application of ancient doctrines of "conversion" to intangible bits always makes me queasy, and it's led to some confused jurisprudence. In this case, the court sidesteps all of that doctrinal messiness for the simple reason that the customer never obtained ownership of the code.

This is really basic copyright law. Customers who want ownership of the work done by vendors need to spell that out in a written agreement. No written agreement specifying customer ownership, no customer ownership--it's that simple. The court says the customer didn't properly obtain ownership in the written customer-vendor agreement, so the vendor had retained copyright title to its developed code all along, and the customer never had title to be converted.

As usual, so many problems are completely avoidable through proper communication through written agreements and amendments between customers and vendors. Some other obvious observations here:

* it's hard to imagine many web development disputes that are worth taking to a state supreme court, especially one where the outstanding bill was about $5k. <LI>* if you are a web developer's customer and you want to own the developed code, you have to say so in a written agreement <LI>* and, if you want a copy of your website's code, make sure you say so in the contract AND actually get a copy! <LI>* if you are a web developer, you might keep customers happier if you keep every version of their website's code instead of tossing old versions. <LI>* t h i s dispute would have be governed by U.C.C. 2B or UCITA if either were the law of Indiana. I wonder to what extent the new ALI Principles on the Law of Software Contracts (acknowledged in the opinion) will help resolve future disputes like this.

While the customer lost the battle here, the issue of when electronic records are subject to conversion doctrines is hardly going away. This

court reaches the sensible result that a putative owner gets no protection from conversion unless he/she actually has title to the asset. Read literally, though, I wonder if this ruling could undercut claims over conversion of virtual world assets? After all, a virtual world asset holder may rarely have clear title to the asset; certainly the holder won't be the copyright owner of the asset. Perhaps the analysis will be different in situations where a third party (the virtual world operator) allocates "title" within its own titling system to users--it might still be possible to deprive an asset holder of "title" within that asset system even if the asset holder would have no conversion claim against the virtual world operator if the operator takes the exact same steps to deprive the asset holder.

Stop Saying "We Can Amend This Agreement Whenever We Want"!

Citation: *Harris v. Blockbuster Inc.*, 2009 WL 1011732 (N.D. Tex. Apr. 15, 2009).

This case is part of the legal detritus from the Facebook Beacon program. As you recall, Facebook Beacon included purchases from third party e-commerce sites into the buyer's Facebook status reports. This required the e-commerce sites to report Facebook users' purchases back to Facebook. A Blockbuster user claimed that Blockbuster's reports to Facebook violated the Video Privacy Protection Act, which prevents disclosures of PII about video customers without their consent. (Beacon did have an opt-out of debatable efficacy). Blockbuster moved to compel arbitration of this lawsuit based on the mandatory arbitration clause in Blockbuster's user agreement.

Blockbuster used an industry-standard and entirely typical introductory clause to its user agreement, which said:

> **Blockbuster may at any time, and at its sole discretion, modify these Terms and Conditions of Use, including without limitation the Privacy Policy, with or without notice. Such modifications will be effective immediately upon posting. You agree to review these Terms and Conditions of Use periodically and your continued use of this Site following such modifications will indicate your acceptance of these modified Terms and Conditions of Use. If you do not agree to any modification of these Terms and Conditions of Use, you must immediately stop using this Site.**

This industry-standard and entirely typical clause does not fare well in this courtroom. Among other defects, the judge notes that "there is nothing in the Terms and Conditions that prevents Blockbuster from unilaterally changing any part of the contract other than providing that such changes will not take effect until posted on the website." As a result, the court deems the arbitration clause "illusory," an odd Texas law descriptor that appears to be a cousin of lack of consideration.

I could wax philosophic about the ontological meaning of a "contract" that one party can amend unilaterally at any time without notice. However, I'd rather focus on the simple practical implication from this ruling. I've never been a fan of the language Blockbuster used, and I had hoped many websites would reconsider the language after the Ninth Circuit trashed such provisions in 2007 in *Douglas v. U.S. Dist. Court for Cent. Dist. of California (Talk America)*, 495 F.3d 1062 (9th Cir. 2007), *cert. denied*, 128 S.Ct. 1472 (2008). Yet, these clauses are still ubiquitous, even at big websites that "should know better," so let me boil it down for you into a single all-caps mantra:

> **STOP PUTTING CLAUSES INTO YOUR CONTRACTS THAT SAY YOU CAN AMEND THE CONTRACT AT ANY TIME IN YOUR SOLE DISCRETION BY POSTING THE REVISED TERMS TO THE WEBSITE**

This language has a significant risk of killing the entire contract, which would strip away a lot of very important provisions that should be/need to be in the contract. So far Blockbuster has only lost its mandatory arbitration clause, but it's possible other important risk management clauses (warranty disclaimer, liability limits, dollar caps, etc.) will similarly fall. If those clauses fail, let the plaintiff feasting begin!

I recognize that weaning ourselves from very flexible amendment language leaves us as drafters with few good options to modify online user agreements over time. However, I got the following email from a reader proposing a good alternative to current amendment notification processes: "To avoid the spam-filter problem, the provider could give notice via an RSS feed as well, and then disclaim like crazy about the problems with the email option (which would indeed simply be an option -- a link to a page where users can sign up to receive notices)." I love this idea! RSS is a true opt-in with few of the challenges of email.

Twitter, Email and Brand Engagement

Recently, in an interview with a reporter, I extolled the virtues of Twitter as a tool for brands to keep in touch with and engage their customers. The reporter responded by asking why brands would choose Twitter to engage customers instead of email, which companies have been using successfully for many years. I thought this question raised important issues about online marketing, so I thought it would be worth exploring the differences here.

Let's start with some basics. I am a big fan of email marketing. Like many of you, I have voluntarily signed up for numerous commercial email newsletters/announcement. I also get unrequested email from companies I've dealt with; I look at some of these, I ignore others, and occasionally I get so fed up that I blacklist the sender or report it as spam. I also get spam, LOTS of spam, but it doesn't bother me too much. Gmail has a good spam filter and it only takes a minute or two a day to sort, review and delete the spam.

However, as a recipient, email has some downsides. Most obviously, it is not always easy to unsubscribe. I remain amazed in this post-CAN-SPAM era by how often email unsubscriptions don't work. The link may be down, or my opt-out simply doesn't stick technologically, or the sender just ignores me. This is true even for senders who are involved in the legal industry and are spamming lawyers who love to bring lawsuits (never a wise move). If I were a litigious plaintiff, I would have no problem finding plenty of defendants.

Email also has the downside that the sender has my email address and may share it with others who are going to clutter up my in-box. With a good spam filter, this extra unwanted email isn't a huge problem, but the mere threat of subsequent email deluges can give me pause about whether or not I trust a website enough to give them my email address. (As you can appreciate, the website's privacy policy is a complete non-factor in my trust determination).

From the sender's standpoint, email is a huge pain. It is more heavily regulated than other marketing media, and complying with the regulations (such as providing a reliable opt-out mechanism) is costly and filled with litigation risks. Perhaps more importantly, email can be reported or killed as spam at several steps along the way, and the sender can be tagged as a spammer as well for all future messages. So, for example, a big website's email distribution of an announcement about a new user agreement or privacy policy--a completely legitimate communication between a site and its users--is almost certain to prompt a flurry of unsubscribes, emails from users who insist to their IAPs and email service providers that they are being spammed (even though they often just forgot about the relationship), and lots of bouncebacks from dead email addresses that may cause some IAPs/email service providers to blacklist the sender as a spammer. Plus, a bunch of users will never see the message at all because it goes into their spam folder. (Recall, for example, that AT&T spam-foldered its own contract amendment announcement). These are not exactly the hallmarks of an effective communication technology.

Contrast the user experience with Twitter. More than anything, Twitter is a no-risk, opt-in

communication tool for consumers to listen to marketers. I can follow a brand at Twitter any time, and more importantly, I can unfollow at any time too. Plus, there isn't any risk that the brand I'm following will ignore my unsubscribes or pass along my Twitter username to spammers. When I unfollow, the relationship is completely over *on my terms*.

From the brand's standpoint, Twitter has none of the baggage of email marketing. No spam folders to fear, no unsubscribes to manage, no CAN-SPAM. Sure, Twitter's tight character restriction mostly limits marketers to headlines, but frankly this isn't all that different from maximizing email subject lines to get email recipients to open the email.

Twitter has one other really important benefit for brands. Folks are often willing to retweet a message--even a commercial message--thereby sharing it to their entire follower base in ways that these same folks would *never* forward a commercial email to hundreds of their friends. And this type of word-of-mouth marketing is the holy grail of marketing because of the extra imprimatur of having the message validated by someone in the reader's social network. The retweeting phenomenon is a powerful traffic driver, and marketers who aren't on Twitter are missing some upside. (Please, marketers, don't even consider shilling or astroturfing or any of those other silly stunts to generate faux word-of-mouth marketing; if you have a good offering, you really don't need to disrespect people that way).

One final point: RSS offers many of the same benefits as Twitter in terms of reader empowerment, although it does not have the same retweeting upside. In particular, RSS is a true opt-in like Twitter. The website doesn't get my email address, and whenever I unsubscribe from the RSS feed in my RSS reader, it's over.

For example, RSS is a great option for websites to allow users to learn about changes to user agreements and privacy policies on a true opt-in basis. In this respect, RSS is so much better than email. Consider, for example, DoubleClick's privacy policy, which offers users the opportunity to learn about privacy policy amendments by signing up to an email list. (DoubleClick will rarely have the email address already because it doesn't have direct privity with users). DoubleClick's option is a more enlightened practice than most similar web services, but still, no thanks. If I don't trust DoubleClick's privacy practices to begin with, I'm not going to give them my email address with the risk that they will spam the crap out of it and pass it along to others who will spam the crap out of it too.

Of course DoubleClick promises not to do this, but the whole point is that those promises mean nothing to the people who don't trust DoubleClick to begin with. On the other hand, if DoubleClick offered an RSS feed to announce modifications to its privacy policy, then I could subscribe to its notifications with no spam risk at all.

I'm so enamored with RSS as a superior notification tool for announcing privacy policy and user agreement amendments that I will be recommending it to all of my clients as a supplement to other notification options. I hope you'll consider doing the same.

47 U.S.C. §230 Can Support 12b6 Motion to Dismiss

Citation: *Gibson v. Craigslist,* 2009 WL 1704355 (S.D.N.Y. June 15, 2009).

In my analysis of the *Barnes v. Yahoo* case, I criticized the Ninth Circuit for concluding that 47 U.S.C. §230 was an affirmative defense (and thus could not support a 12b6 motion to dismiss) without proper briefing or analysis. First, this was sloppy work by the court. Second, the elimination of a 12b6 possibility for the defendants creates a real risk that defendants will be exposed to expensive and time-consuming discovery to eliminate plainly meritless cases.

Today's case does a competent job reviewing whether or not 47 U.S.C. §230 can support a 12b6 motion to dismiss. Unlike the Ninth Circuit, it actually cites and discusses the numerous cases in the area although, remarkably, it does not cite or address the *Barnes v. Yahoo* case! The court reaches the sensible positions that (1) 47 U.S.C. §230 does support a 12b6 motion, (2) as a result,

the plaintiff was not entitled to discovery, and (3) the case should be dismissed.

Substantively, this lawsuit is brought by a shooting victim who claims that the shooter bought the gun via Craigslist. The complaint argues that Craigslist had a duty to prevent the sale of guns to future criminals and therefore Craigslist breached the duty. This argument is similar to the *Doe v. MySpace* cases in which the plaintiffs argued that MySpace had a duty to police its website "premises" to prevent online communications that lead to offline crimes. The plaintiff's argument here fares no better here than it did in the *MySpace* cases. 47 U.S.C. §230 precludes the imposition of liability for any breach of duty by failing to police its users' communications (putting aside the also-relevant inquiry of whether Craigslist could have any duty that would have prevented this offline tragedy).

The plaintiff tries to get around Section 230 by arguing it's just trying to hold Craigslist accountable as a "business" rather than as a speaker or publisher of third party content, but the court rejects this goofy argument as "unpersuasive."

Ninth Circuit Helpfully Amends Barnes v. Yahoo Opinion

Citation: *Barnes v. Yahoo, Inc.*, 05-36189 (9th Cir. Amended Opinion June 22, 2009).

The Ninth Circuit has issued an amended opinion in last month's *Barnes v. Yahoo* opinion. The amended opinion makes two changes to the initial opinion, both of significant value.

First, the opinion deletes the entire old section II, a two paragraph section where the panel declared that, under Ninth Circuit law, 47 U.S.C. §230 is an affirmative defense that could not support a 12b6 motion to dismiss. That discussion was poorly researched, sloppy and completely gratuitous. Rather than try to fix the section, the panel wisely decided just to kill it. This still leaves open the possibility that a district court will reject a Section 230 defense to a 12b6 motion, although I think the better result is that 230 can support a 12b6 motion as the *Gibson v. Craigslist* case (discussed above) recently held.

Second, the panel added a new footnote to its recap of the prima facie elements of a 47 U.S.C. §230 defense. In my initial critique of the opinion, I excoriated the panel for saying, in plain language, that 47 U.S.C. §230 only applied to state law claims. To fix this obvious error, the panel added the following footnote:

> **We limit our restatement of section 230(c)(1) to state law claims because we deal in this case with state law claims only. We have held that the Amendment's protection also extends to federal law causes of action, *see, e.g., Fair Housing Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157 (9th Cir. 2008) (en banc) (applying the Amendment to a cause of action under the Fair Housing Act, 42 U.S.C. § 3601 *et seq.*). Because no federal law cause of action is present in this case, we need not decide how or whether our discussion of section 230(c)(1) would change in the face of such a federal claim.**

I don't know why the last sentence of the footnote is there. Everyone knows that the 230(c)(1) analysis doesn't change one bit between federal and state law claims. Nevertheless, this footnote should eliminate any efforts by plaintiffs' lawyers to misuse the prior unnecessarily sloppy language.

Both of the changes in this amended opinion were directly responsive to the requests Yahoo and its amici made. I suspect both groups are pleased with these changes. I certainly am, although I remain disappointed that the entire exercise was necessitated by the panel's sloppy work up-front. Given that this is the second time in 2 years that the Ninth Circuit has had to fix badly drafted 47 U.S.C. §230 opinions, I remain (overly?)optimistic that the Ninth Circuit will be more careful with its Section 230 jurisprudence in the future.

In conjunction with the amendments, the Ninth Circuit rejected both sides' request for an en banc hearing, although the amendments were so responsive to the defense requests that they largely mooted the defense's requests. (My intuition is

that the plaintiffs never expected to get an en banc hearing but made their request just because Yahoo and the amici had put an en banc hearing in play). I would be surprised if there are further appeals to the Supreme Court at this point. As a result, I believe this case is now effectively ready for further proceedings on remand on the promissory estoppel claim. Personally, from the limited material I've seen, Yahoo might find it prudent to cut short further proceedings and settle up rather than have its choices scrutinized too carefully. So I would not be surprised if this amended opinion prompts a settlement soon.

Anti-Spyware Company Protected by 47 USC 230(c)(2)

Citation: *Zango, Inc. v. Kaspersky Lab, Inc.,* 2009 WL 1796746 (9th Cir. June 25, 2009).

The case involves Kaspersky, an anti-spyware software vendor, and Zango, the former purveyor of adware (I say "former" because Zango shut down a few months ago). Kaspersky classified Zango's software as adware and did some other things that allegedly interfered with Kaspersky users' ability to download and enjoy Zango software. Zango sued Kaspersky, and Kaspersky defended on Section 230(c)(2) grounds.

Note: 47 U.S.C. §230(c)(2) is the underlitigated/under-discussed sibling of 230(c)(1), which provides nearly absolute immunity for third party online content and actions.

In my opinion, Section 230(c)(2) fairly clearly protects all types of online filtering decisions, and this panel confirms that it protects anti-spyware classifications. As the court concludes:

> **a provider of access tools that filter, screen, allow, or disallow content that the provider or user considers obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable is protected from liability by 47 U.S.C. § 230(c)(2)(B) for any action taken to make available to others the technical means to restrict access to that material.**

While I think this is the right result, both normatively and descriptively, 230(c)(2) is not exactly the best-drafted statute, and this panel (being the first appellate court to work through the language) appeared to struggle with some of its frayed edges.

For example, to become eligible for Section 230 protection, the defendant must be a provider or user of a service that "provides or enables computer access by multiple users to a computer server." [In this case, Kaspersky didn't claim it was a user.] How does this language apply to an anti-spyware software provider? Typically, anti-spyware software phones home for new spyware definitions, but if a phone-home capability qualifies for 230 protection, then many/most software vendors should qualify (so long as they offer some filtering capability). I'm personally OK with that result, but I suspect it takes the statute beyond the drafters' initial intent.

The panel also sidestepped some other drafting problems in Section 230(c)(2), including:

* Does it immunize decisions to filter other software, as opposed to filtering content? The drafting clearly meant to immunize filters of porn and similar kid-unfriendly content, but the language doesn't apply as clearly to software filtering.
* Must the filtering provider make its categorizations in good faith? The court ducks this question. However, Judge Fisher's concurrence expresses concern that Section 230(c)(2) might literally protect a vendor's anti-competitive or capricious blocking. He gives an example of "a web browser configured by its provider to filter third-party search engine results so they would never yield websites critical of the browser company or favorable to its competitors. Such covert, anticompetitive blocking arguably fits into the statutory category of immune actions." I agree with this, although I'm also confident that any such browser provider would lose its customer base if such biases were ever publicly exposed. Therefore, legal liability may not be necessary to discourage this behavior.

Ultimately, this ruling may not affect the litigants very much, as Zango has already gone belly-up, making this effectively an advisory opinion. However, I think this ruling is important for everyone else for two reasons:

First, the Ninth Circuit's last two Section 230 opinions (*Roommates.com* and *Barnes v. Yahoo!*) have exhibited some hostility to expansive Section 230 readings. In refreshing contrast, this opinion gives a robust interpretation to Section 230's immunizations.

Second, this opinion is terrific news for vendors of anti-spam/anti-spyware/anti-virus services. Although we have long suspected that they would be protected under 230(c)(2), this opinion codifies their immunization as Ninth Circuit law. As a result, these vendors should continue to have a high degree of freedom to make judgments about how to best serve their customers. On the flip side, this opinion confirms that anyone blacklisted by these software vendors can't use judicial proceedings to change the classification. Fortunately, most reputable vendors offer an extra-judicial mechanism to correct their misclassification errors.

It remains less clear if this opinion protects search engines for their ranking determinations. The statutory words interpreted in this opinion aren't germane to search engines. Even so, the panel's broad reading of Section 230(c)(2) can't be bad news for the search engines.

Advertising Industry Publishes Self-Regulatory Principles for Online Behavioral Data Collection

BY ROBERT J. DRISCOLL, PAUL GLIST & JENNIFER SMALL*

Robert J. Driscoll (robertdriscoll@dwt.com) is a partner in the New York City office of Davis, Wright & Tremaine. Paul Glist (paulglist@dwt.com) is a partner and Co-Chair, Communications, Media & Information Technology Practice, in the firm;'s Washington, D.C. office. Jennifer Small (jennifersmall@dwt.com) is an associate in the firm's Seattle office.

Introduction

On July 2, 2009, a group of advertising industry associations published the Self-Regulatory Principles for Online Behavioral Advertising—a set of guidelines concerning the collection and use of online behavioral data by advertisers, service providers, publishers and ad networks.

The principles, drafted by the American Association of Advertising Agencies (4A's), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), the Interactive Advertising Bureau (IAB) and the Council of Better Business Bureaus (BBB), focus on the areas that the Federal Trade Commission (FTC) has identified as desirable for industry self-regulation. The principles set forth recommended practices for providing consumers with greater control over online behavioral advertising.

These proposed self-regulatory principles arise against a backdrop of growing political and consumer awareness of privacy issues. FTC Chairman Jon Leibowitz has twice warned the industry that it is facing the "last clear chance" to avoid specific

governmental regulation. The FTC has stepped up enforcement action in the area, recently proposing an order against Sears that treats formal notices of Web tracking buried in fine print as "unfair" or "deceptive" under current law.

This article provides a brief overview of the new principles. Businesses involved in online behavioral advertising should be aware of them and consider taking steps toward their implementation.

Of particular note is an enhancement of consumer notice and education about the collection and use of predictive profiling information, with new, easier-to-use tools for consumers to "opt out" of such collection and use by online ad networks. In addition, the principles propose more significant restrictions on service providers—specifically, Internet service providers and providers of desktop application software such as browsers and tool bars—who would be permitted to engage in the collection and use of data for online behavioral advertising purposes only on an "opt in" basis.

The principles do not address display advertising or contextual advertising; rather, they focus on advertising targeted to the user based upon data regarding that user's activities across various Web sites, a practice that has attracted considerable political attention.

Proposed Requirements

Transparency

Online behavioral advertising will be accompanied by enhanced notice to consumers. Among other things, the principles contemplate that a uniform link or icon indicating that behavioral data is being collected will be displayed in or around behavioral ads. In addition, ad networks and other entities that collect and use data from others' Web sites would be required to include notices of their online behavioral advertising practices on their Web sites, along with a mechanism for consumers to opt out of the collection and use of behavioral data. Service providers would also be required to provide online notices of their behavioral advertising practices, and Web sites at which behavioral data is collected would be required to display links to the ad networks' notices.

Consumer Control

The principles require entities involved in online behavioral advertising to provide users with a means of controlling the collection and use of data relating to them. Ad networks could satisfy this obligation by providing a means for consumers to opt out of such data collection and use. Service providers, on the other hand, would be prohibited from collecting or using data for online behavioral advertising purposes without securing affirmative consumer consent, i.e., by deploying an opt-in mechanism.

Data Security

Data will be reasonably secured and discarded when no longer necessary to fulfill a legitimate business or law enforcement purpose. This principle extends to offer reasonable assurances that the anonymization process will prevent the re-identification of anonymized profiles.

Material Changes

Consent is required for any retroactive material change in the use of collected data.

Sensitive Data

Children known to be under 13 are provided additional protections, as is health and financial data. The principles note that what is "sensitive" information may change over time.

Accountability

Enforcement of the principles will be handled principally by nongovernmental bodies, perhaps analogous to the Children's Advertising Review Unit of the Better Business Bureau with respect to children's advertising issues. Enforcement mechanisms may include internal and third-party monitoring and self-reporting systems, and possible reports to the applicable government agencies in the event of an uncorrected violation.

Education

Participants are encouraged to educate individuals and businesses about online behavioral

advertising. It has been reported that industry groups expect to conduct a large educational campaign—on the order of 500,000,000 impressions—over the next 18 months.

Conclusion

Currently key House members are drafting new legislation on online privacy. We expect that even if such legislation is pursued, it may still provide room for effective self-regulatory programs to operate. In the meantime, the BBB will spearhead implementation of the Self-Regulatory Principles for Online Behavioral Advertising, with an implementation program expected to be launched by early 2010.

TJ Maxx Settlement

Requires Creation of Information Security Program and Funding of State Data Protection and Prosecution Efforts

BY TARA M. DESAUTELS & JOHN L. NICHOLSON

Tara M. Desautels (tara.desautels@pillsburylaw.com) is a Senior Associate in the San Francisco office of Pillsbury Winthrop Shaw Pittman LLP. John L. Nicholson (john.nicholson@pillsburylaw.com) is counsel in the firm's Washington, D.C. office.

TJX (the parent company of TJ Maxx and Marshalls) recently settled an action with 41 state Attorneys General arising out of a 2006 security breach affecting millions of credit cardholders. An information security program required by the settlement covers a significantly broader collection of information than the Payment Card Industry Data Security Standards (PCI DSS) and may serve as a de facto minimum standard for information security compliance. Also, the settlement's funding of a Data Security Trust Fund anticipates future enforcement activities by the states and creates a precedent for states to look to future breaches as a source of continued funding.

Background

On December 18, 2006, TJX initiated an investigation after discovering suspicious software on its computer systems. That investigation led to the shocking discovery that for 18 months prior, hackers had stolen information dating as far back as 2002 from more than 94 million credit and debit cards. TJX reported the security breach to U.S. state and federal authorities and government authorities in Canada, France, and the United Kingdom. The related investigation initiated by a group

of state Attorneys General revealed that TJX had failed to address the security flaws identified in a 2004 internal audit that revealed vulnerabilities concerning firewalls, encrypting cardholder data, uploading antivirus software, and regularly testing security systems.[1] Litigation immediately followed, as did evidence that TJX was not compliant with nine of the twelve PCI DSS requirements covering encryption, access controls and firewalls.[2]

On June 23, 2009, TJX settled the action with 41 state Attorneys General for $9.75 million.[3] This settlement agreement follows the 2007 settlements of the consolidated consumer class action[4] and an action initiated by Visa, Inc.[5] But unlike the prior settlement agreements, in addition to monetary payments, the June 23 agreement requires TJX to implement a comprehensive "Information Security Program" and fund future state data protection efforts as part of "the most comprehensive relief achieved to date following a data breach investigation."[6]

The Terms

The settlement agreement between TJX and the states (known as the "Assurance") breaks down the $9.75 million payments into cost reimbursement and future data protection funding:[7]

- $5.5 million will be dedicated to data protection and consumer protection efforts by the states;
- $1.75 million will reimburse the states for their costs and fees incurred in the investigation; and
- $2.5 million will fund a "Data Security Trust Fund" to be used by the state Attorneys General to "advance enforcement efforts and policy development in the field of data security and protecting consumers' personal information."

Within the next 120 days, TJX must also "implement and maintain a comprehensive Information Security Program that is reasonably designed to protect the security, confidentiality, and integrity of Personal Information." The Assurance uses a definition of Personal Information that is generally consistent with numerous state data breach notification laws and is significantly broader than the definition of "cardholder data" used by the PCI DSS. According to the Assurance,

> **"Personal Information" shall mean any TJX record, whether in paper, electronic or other form, containing nonpublic personal information about a Consumer collected in connection with a Transaction, including, but not limited to, any (1) Consumer's name, address, or telephone number, in conjunction with the Consumer's Social Security number, driver's license number, financial account number, or credit or debit card number; (2) Consumer's user name and passphrase used to authorize Transactions over the Internet; or (3) sensitive payment card authentication data, which shall mean (a) Primary Account Number ('PAN'); (b) cardholder name, card expiration date, service code, Social Security number, date and place of birth, or mother's maiden name, in conjunction with PAN; or (c) full magnetic stripe data, CVC2/CVV2/CID, or PIN or PIN block; or (4) other information required to be protected by state or federal law.[8]**

By contrast, under the PCI DSS, cardholder data is (1) the PAN and (2) the cardholder's name, the card expiration date and the service code, but only to the extent associated with the PAN. The Assurance also defines Cardholder Data in a manner consistent with the PCI DSS, but most of TJX's specific requirements under the Assurance are express as covering "Personal Information, including Cardholder Data." It is this structure that makes the information security obligations under the Assurance so much broader than those required solely by the PCI DSS.

The Assurance specifies that TJX's Information Security Program must include – at a minimum – certain administrative, technical, and physical safeguards that are listed in the Assurance. Although the information covered by the Assurance is broader than that required by PCI DSS, for the purposes of comparison, each of the Assurance's requirements is mapped against the relevant PCI DSS requirement(s) in the following list:

	Assurance Requirement	PCI DSS Requirement
1.	The designation of an employee or employees to coordinate and be accountable for the Information Security Program;	PCI DSS 12.5 requires a company to "Verify the formal assignment of information security to a Chief Security Officer or other security knowledgeable member of management."
2.	The identification of material internal and external risks to the security, confidentiality and integrity of Personal Information that could result in unauthorized disclosure, misuse, loss, alteration, destruction or other compromise of such information and assessment of the sufficiency of any safeguards in place to control these risks. The risk assessment should consider risks in each area of relevant operation, including, but not limited to (a) employee training and management; (b) information systems, including network and software design, information processing, storage, transmission, and disposal; and (c) prevention, detection, and response to attacks, intrusions, or other system failures;	PCI DSS Requirement 12 requires companies to "Maintain a policy that addresses information security for employees and contractors." As part of that requirement, PCI DSS 12.1 requires companies to "Establish, publish, maintain, and disseminate a security policy that accomplishes the following: … Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment."
3.	The design and implementation of reasonable safeguards to control the identified risks through risk assessment and regular testing and monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;	PCI DSS 12.2 requires companies to "Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures)." PCI DSS 12.6 requires an annual (or more frequent) formal security awareness program for employees, and PCI DSS 12.9 requires the implementation of an incident response plan, including for alerts from intrusion detection systems, intrusion-prevention systems and file-integrity monitoring systems.
4.	The implementation and evaluation of any modification to the Information Security Program, in light of the results of the testing and monitoring of any material changes to TJX's operation or business arrangements, or any other change in circumstances that TJX knows or has reason to know may have a material impact on the effectiveness of the Information Security Program.	As part of the maintenance of the security policy required by PCI DSS 12.1, PCI DSS 12.1.3 requires companies to include a "review at least once a year and updates when the environment changes."

Because of the increased breadth of the information covered by the Information Security Program, items 2-4 in the preceding table may require TJX to cover information and operations previously considered outside of the coverage of its PCI DSS program.

The Assurance further requires that TJX implement the following security provisions (to the extent it has not already done so). As with the preceding table, for the purposes of comparison, each of the Assurance's requirements is mapped against the relevant PCI DSS requirement(s):

	Assurance Requirement	PCI DSS Requirement
1.	Replace or upgrade all Wired Equivalent Privacy ("WEP") based wireless systems in TJX's retail stores with wired systems or with Wi-Fi Protected Access ("WPA") or wireless systems at least as secure as WPA.	PCI DSS 2.1.1 requires a company to "ensure that all wireless networks implement strong encryption mechanisms (for example, AES)" and that "Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)…").
2.	Not store or otherwise maintain on its network subsequent to the authorization process the full contents of magnetic stripe of a credit or debit card, or of any single track of such a stripe, or the CVC2/CVV2/CID, or the PIN or PIN block of any card. TJX may retain a portion of the contents of the magnetic stripe of a credit or debit card on its network subsequent to the authorization process for a period of time for legitimate business, legal or regulatory purpose(s), but any such Cardholder Information must be securely stored in encrypted form, be accessible only to essential personnel, and retained for no longer than necessary to achieve the business, legal or regulatory purpose;	These requirements are covered by PCI DSS 3.2.1 ("Do not store the full contents of any track from the magnetic stripe …"), 3.2.2 ("Do not store the card-verification code or value … used to verify card-not-present transactions."), 3.2.3 ("Do not store the personal identification number (PIN) of the encrypted PIN block."). The encryption, storage and access requirements are covered in PCI DSS 3.1 and 3.4 – 3.6.
3.	Segment the network-based portions of the TJX computer system that store, process, or transmit personal information from the rest of the TJX computer system through firewalls, access controls, or other appropriate measures;	These requirements are covered by, among others, PCI DSS 1.2 ("Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.") and 1.3 ("Prohibit direct public access between the Internet and any system component in the cardholder data environment.").
4.	Implement security password management for the portions of the TJX computer system that store, process, or transmit Personal Information, including Cardholder Information, such as, where appropriate, strong passwords and, with respect to remote access to the network, two-factor authentication;	PCI DSS 8.2 requires "In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: password or passphrase; two-factor authentication…" PCI DSS 8.3 requires companies to "Incorporate two-factor authentication for remote access … to the network by employees, administrators, and third parties."
5.	Implement security patching protocols for the portions of the TJX computer system that store, process or transmit Cardholder Information;	PCI DSS 6.1 requires companies to "Ensure that all system components and software have the latest vendor-supplied security patches installed." The PCI DSS goes further to also require all critical security patches to be installed within one month of release.
6.	Use Virtual Private Networks ("VPNs") or, where appropriate, encrypted transmissions, or other methods at least as secure as VPNs for transmission of Personal Information, including Cardholder Information, across open, public networks;	PCI DSS 4.1 requires the use of "strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks."

7.	Install and maintain appropriately configured antivirus software on the portions of the TJX computer system that store, process or transmit Personal Information, including Cardholder Information, and that are commonly affected by viruses;	This requirement is covered by PCI DSS 5.1 ("Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)"), 5.1.1 ("Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.") and 5.2 ("Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.")
8.	Implement and maintain security monitoring tools such as intrusion detection systems and other devices to track and monitor unauthorized access to the portions of TJX's computer systems that store, process and transmit Personal Information, including Cardholder Information. Conduct regular testing or monitoring of the key systems and procedures used to protect Personal Information, including Cardholder Information; and	PCI DSS Requirement 10 requires companies to "Track and monitor all access to network resources and cardholder data." Requirement 11 requires companies to "Regularly test security systems and processing."
9.	Implement Personal Information access control measures for the portions of TJX's computer system that store, process and transmit Personal Information, including Cardholder Information. Access control measures include: (a) limiting physical and electronic access to Cardholder Information on a need-to-know basis; (b) assigning unique user IDs to persons with access to Cardholder Information; and (c) generating logs or other inventories of the user accounts on the portions of TJX's computer system used to store, process or transmit Cardholder Information.	PCI DSS section 9 covers physical security with regard to cardholder data, including PCI DSS 9.1 ("Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment."), 9.6 ("Physically secure all paper and electronic media that contain cardholder data."), and 9.9 ("Maintain strict control over the storage and accessibility of all media and conduct media inventories at least annually.") PCI DSS 7.1 requires companies to "Limit access to system components and cardholder data to only those individuals whose job requires such access." Assignment of user IDs is covered by PCI DSS 8.1 ("Assign all users a unique ID before allowing them to access system components or cardholder data."), and, as noted above, PCI DSS Requirement 10 requires companies to "Track and monitor all access to network resources and cardholder data."

The Attorneys General will issue TJX a compliance certification only after TJX provides satisfactory documentation of its implementation of all of these security measures. Given the breadth of the definition of "Personal Information" used in the Assurance, it seems unlikely that a successful audit by a PCI DSS Qualified Security Assessor, by itself, would satisfy the requirements. Under the Assurance, TJX will be required to obtain a CISSP (Certified Information System Security Professional) or CISA (Certified Information Systems Auditor) third-party assessment and report of its security and compliance efforts within the next 180 days and bi-annually thereafter for the next 20 years. Since TJX's regular PCI DSS audits may not be sufficient, this could represent a significant additional cost to TJX. If TJX has outsourced any functions to third parties that must

be covered by such an audit, TJX may need to determine whether the contracts with those third parties will permit the level of detailed investigation required. In some cases, TJX may be caught between the "rock" of the state Attorneys General and the "hard place" of a supplier that does not want to permit auditing of its services (except in exchange for a significant payment).

In addition, if TJX discovers a future security breach, it must also notify the Attorneys General within 10 business days (or earlier if required by applicable law) after mailing notice to resident consumers pursuant to each of the affected states' security breach notification laws.

Finally, TJX has agreed to participate in substantial payment card system pilot programs and security enhancements. For the next two years, TJX will, if invited, participate in pilot programs testing new security-related payment card technology, such as "chip-and-PIN" technology. TJX will also take proactive steps within the next 180 days to encourage the development of new security-based technologies within the payment card industry to encrypt cardholder information.

What the TJX Settlement Means for You

The TJX Settlement is a warning. All companies maintaining personal information that meets the definition used in the Assurance (i.e., name, address or telephone number in combination with Social Security Numbers, drivers license numbers, credit/debit card account numbers or other similar account/identification numbers, as well as the information specifically covered by the PCI DSS, in paper, electronic or other forms) – whether for consumers, employees, or third-parties – must implement a secure information protection program with regular auditing procedures. In setting up such a program, the specifics set forth in the TJX Assurance and the PCI DSS can serve as a guide, but companies must tailor their program to their particular circumstances.

Companies that have outsourced any data processing to third parties should review the security obligations under those contracts to determine whether the service provider is obligated to meet requirements that comply with the Assurance and whether the company is permitted to audit the service provider's compliance. Companies in the process of negotiating (or renegotiating) such agreements should include these security and audit obligations in the terms of the contract.

Companies should also keep in mind that the states now have an additional $8 million among them allocated specifically to advance data and consumer protection efforts – which means increased enforcement of state data breach notification and consumer protection laws. Once the Data Security Trust Fund is established, companies can expect states to use such increased enforcement efforts to secure future funding, which not only makes state Attorneys General look proactive to their constituents, but does so in a manner that pays for itself. Payments into the Fund may become the rule rather than the exception.

In the world of security breaches, the question is not, "Will you have a breach?" It is, "When will you have one?" When you discover that inevitable security breach, your company must have the appropriate incident response procedures in place, along with certified evidence of all of your regular, prior, and audited compliance efforts. The TJX Settlement, including the broad definition of information to be covered by a company's information security program, may now serve as the baseline for such programs, and companies that fall short of meeting these obligations may fare far worse than TJX.

1. *See* June 23, 2009 Press Release, "Brown Forces Parent Company of TJ Maxx and Marshall's to Block Credit Card Hackers," Office of the Attorney General, State of California.
2. *See* Brenner, "Don't blame PCI DSS for TJX troubles, IT pros say," SearchSecurity.com, Nov. 5, 2007.
3. The participating states are: Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington, West Virginia, Wisconsin and the District of Columbia.

4. On November 14, 2007, parties reached a proposed settlement agreement in the Consolidated Consumer Class Action approved by the United States District Court for the District of Massachusetts on September 2, 2008. The settlement agreement provided for compensation to injured consumers through vouchers or checks-in-lieu, credit monitoring, identity theft insurance, reimbursements, a one-time sale event, and over $6.5 million in attorneys fees and costs. *In re TJX Companies Retail Security Breach Litigation,* United States District Court, District of Massachusetts, Civil Action No. 07 10162, MDL Docket No. 1838, Dkt. 368.
5. In the November 30, 2007 settlement agreement with Visa Inc., TJX agreed to provide U.S. credit card issuers up to $40.9 million in alternative recovery payments. In a December 20, 2007 press release, TJX announced over 95% of the affected institutions accepted the proposal.
6. *See* June 23, 2009 Press Release, "Attorney General Martha Coakley Announces Multi-State SettlemeCompanies, Inc., Over Massive Data Breach," Office of the Attorney General, State of Massachusetts.
7. See id. and accompanying Assurance, In the Matter of: The TJX Companies, Inc., at http://www.mass.gov/?pageID=cagopressrelease&L=1&L0=Home&sid=Cago&b=pressrelease&f=2009_06_23_tjx_settlement&csid=Cago#materials.
8. Id. at Assurance, In the Matter of: The TJX Companies, Inc., at 4.

Effects of Recent Rulings on the Enforceability of Open Source Licenses

BY ROBERT C. DOWERS & LAURENCE F. PULGRAM*

Robert C. Dowers (rdowers@fenwick.com) is an associate and Laurence F. Pulgram is a partner (lpulgram@fenwick.com) in the San Francisco office of Fenwick & West.

Introduction

Increasingly, software licensors are opting to license their software under non-traditional license arrangements. These license agreements can take a variety of forms, but are most commonly marked by their tit-for-tat approach. For instance, the licensor may make the source code of the software freely available, but may then require licensees to provide attribution of the original licensor or author, to license any modifications made to the code under the same license, or any other requirement the licensor deems appropriate. This family of licenses and their myriad variants, including the General Public License (GPL), are typically referred to as "open source licenses" or "free licenses."

Although the basic principle of freedom of contract gave these licenses some legitimacy, some licensees and licensors may have been reticent to license their software under new conceptual frameworks that had not yet been judged enforceable by a court of law. Two recent groups of cases, *Jacobsen v. Katzer,* 535 F.3d 1373 (Fed. Cir. 2008) (originating in California), and the *BusyBox* cases (originating in the United States Court of Appeals, Second Circuit), have shown that courts are increasingly more willing to uphold these licenses.

Jacobsen v. Katzer Decision

In *Jacobsen*, plaintiff Jacobsen designed software used by model train hobbyists, and licensed the software pursuant to an "Artistic License." This license required the user of the software to provide several attributions to, and identifications of, the origin of the software if the user later integrated the software into his own product. Katzer created his own model train software, integrating Jacobsen's software; he then failed to include the necessary attributions.

Jacobsen brought suit in the U.S. District Court, Northern District of California, and filed for a preliminary injunction, claiming that violation of the Artistic License constituted copyright infringement. Under the United States Court of Appeals Ninth Circuit law, irreparable harm can be presumed in a copyright infringement case; however, a copyright owner who merely grants a non-exclusive license generally waives his right to sue the licensee for copyright infringement over a mere breach of the license. If, however, a license is limited in scope and the licensee acts outside that scope, the licensor can bring an action for copyright infringement.

The district court denied relief, holding that Jacobsen only had an action for breach of contract. It stated that the Artistic License was an "intentionally broad," "non- exclusive license," and the requirement of attribution did not "limit the scope of the license." As such, Katzer's "alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license, but [did] not create liability for copyright infringement where it would not otherwise exist." Thus, there could be no irreparable harm and a preliminary injunction was improper. Jacobsen appealed to the U.S. Court of Appeals for the Federal Circuit. The Federal Circuit reversed and remanded, finding that the Artistic License contained enforceable copyright conditions.

The court's decision centered on whether the terms of the Artistic License were covenants or conditions. If they were covenants (i.e., actions the user promises to do or refrain from as part of their use of the software), then violation of those covenants would give rise only to an action for breach of contract. If, on the other hand, they were conditions (i.e., terms which define the scope of the license itself or are preconditions of effectiveness of the license), then violation of those conditions would constitute use outside the scope of the license, and thus an action for copyright infringement would be possible.

The court examined the plain language of the Artistic License, which stated that "the intent of this document is to state the conditions under which a Package may be copied" (emphasis added). The court also noted that the agreement used the "traditional language of conditions," stating that the rights to copy, modify, and distribute were granted "provided that" the conditions were met.

Finally, the court noted that these conditions "are vital to enable the copyright holder to retain the ability to benefit from the work of downstream users" and that it is irrelevant that there is no direct economic benefit (i.e., because the software is free). The attribution requirements are their own kind of consideration, and "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."

First and foremost, this ruling legitimizes open source licenses. The theory behind commonly-used open source licenses such as the GPL and Creative Commons licenses is that the license sets forth conditions, the violation of which results in unlicensed use of the work. Unlicensed use of the work by the licensee is an infringement of the licensor's copyright, which then gives rise to a copyright infringement action. This ruling essentially affirms the theory upon which these open source licenses were crafted and gives licensors (and licensees) comfort in knowing that the arrangements under which they choose to license software can be enforced if litigated.

Second, the ruling provides important guidance to licensors who wish to license their work under a non-standard license. As the court looked closely at the plain language of the license, it is important for licensors to ensure that their licenses contain the "buzzwords" a court will be looking

for — language setting forth the conditions under which the license is granted, or language stating that certain rights are granted "provided that" certain conditions are met, or are "conditioned on" or "subject to" specific terms.

Finally, the result on remand is instructive. The district court, in its original opinion, did not make any factual findings on the likelihood of irreparable harm; the Federal Circuit remanded with instructions to do so. The district court held that Jacobsen did not show that the harm he suffered was sufficiently "real, imminent, and significant, not just speculative or potential" to obtain injunctive relief, as required by Ninth Circuit jurisprudence.

Although this ruling is both fact-specific and non-precedential, it suggests that licensors should be prepared to demonstrate actual harm they have suffered if they desire injunctive relief, and that conceptual arguments of potential harms may not be sufficient even if the license is otherwise conditioned on performance that did not occur.

Busybox Cases

The B*usyBox* cases followed from a series of complaints filed in 2007 and 2008 in the US District Court for the Southern District of New York. BusyBox is a software application that provides many standard UNIX tools compressed and optimized for use on mobile and embedded devices. BusyBox was released under the GPLv2 license, which requires that redistributors of the BusyBox software provide end users with access to the BusyBox source code. The developers of BusyBox identified seven redistributors of the software who were not complying with the license terms. Specifically, these entities failed to make the BusyBox source code available to the end user.

From September 2007 to July 2008, the BusyBox developers filed complaints against these redistributors in the Southern District of New York. The complaints were notable as being the first copyright infringement cases based on the GPL. The argument made by BusyBox was the same in each complaint. By failing to adhere to the terms of the license, the redistributor's use of the BusyBox software was outside the scope of the license, and thus amounted to copyright infringement.

Each complaint was dismissed after the parties reached a settlement agreement. The settlements were substantially similar. In each case, the redistributor agreed to appoint an "Open Source Software Compliance Officer" to monitor potential licensing issues, to publish the source code and inform their customers of its availability, to pay an undisclosed sum to the plaintiffs, and in one case, agreed to cease distribution of the offending article until the source code was published.

Several interesting results come out of the *BusyBox* cases. Although no court actually ruled on the matter, it does seem likely that the logic of *Jacobsen* would apply if a claim were to reach that stage. The GPLv2 uses conditions, not covenants; it permits redistribution "provided that" the user meets a list of "conditions." The holding in *Jacobsen* would, therefore, likely lead to a favorable result for BusyBox.

Second, it is important for licensees to become familiar with exactly what obligations are imposed upon them by a licensor's chosen license. For example, the GPLv2 license requires that a licensee not only make source code available, but also associated definition files and scripts used to control installation and compilation of the executable. Failure to comply fully with the license terms may lead to the same result as would failure to comply at all. Given that there are a variety of free software licenses available for use by licensors, any potential licensee should look before it leaps.

These cases also highlight the importance of internal communication between various business units. If a software developer uses open source code, it is essential that all relevant parties (legal, corporate communication, and other groups) be aware of this choice in order to avoid potential legal and public relations issues. As shown by the settlement agreements reached in the *BusyBox* cases, failure to do so can result in monetary settlements, temporary cessation of production or shipping, and other business disruptions.

Finally, a common theme throughout the *BusyBox* cases suggests that the licensors attempted to discuss the issue with each licensee prior to

filing the complaint; in each case, their attempts at discussion were rebuffed or ignored, leaving litigation as the only remaining option. Licensees should consider engaging in informal discussions before a licensor feels compelled to pursue litigation, given the *Jacobsen* decision. The risks of ignoring the license are genuine and significant.

Conclusion

Jacobsen and the *BusyBox* cases both reflect a gradual acceptance of non-standard (and, compared to the status quo, radically different) licenses. Both licensors and licensees should obtain some comfort from these cases; licensors know they have the freedom to license their works on terms, which reflect their principles (and that those terms will be enforced by a court), and licensees know that this regime will provide a construct on which to base their conduct. Judicial acceptance of these licenses also threatens to spawn additional litigation, and therefore heightens the need for licensees to be sure they know what terms they are agreeing to, and to coordinate internal compliance prior to being targeted for litigation.

Calendar of EVENTS

September 9, 2009 New York City
September 23, 2009 San Francisco

Technology and Entertainment Convergence 2009: Business and Legal Issues for the Next Stage of "Technotainment"

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

September 21-22, 2009 Chicago
October 22-23, 2009 San Francisco
November 2-3, 2009 New York City

Outsourcing and Offshoring 2009: Protecting Critical Business Functions

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

October 6, 2009 New York City
October 28, 2009 Chicago
December 4, 2009 San Francisco

Electronic Discovery Guidance 2009: What Corporate and Outside Counsel Need to Know

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

October 26-27, 2009 New York City
November 5-6, 2009 Chicago
December 14-15, 2009 San Francisco

Understanding the Intellectual Property License 2009

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

October 29-30, 2009 San Francisco

Intellectual Property Law Institute 2009 (15th Annual)

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

November 12-13, 2009 New York City

Communications Law in the Digital Age 2009

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

November 18, 2009 New York City
December 9, 2009 San Francisco

Open Source Software 2009: Benefits, Risks and Challenges for Software Users, Developers and Investors

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

Cyberspace LAWYER

West Legalworks
195 Broadway, 9th Floor
New York, NY 10007

FIRST CLASS
U.S.POSTAGE
PAID
WEST

Cyberspace LAWYER

West Legalworks
195 Hudson Street, 9th Floor, New York, NY 10007
Phone: 212-337-8444 or 800-308-1700
Fax: 212-337-8445
E-mail: west.legalworksregistration@thomsonreuters.com
Web: www.westlegalworks.com

WEST®

YES! Rush me ***Cyberspace Lawyer*** and enter my one-year trial subscription (11 issues) at the price of $451.00. After 30 days, I will honor your invoice or cancel without obligation.

Name _____

Company _____

Street Address _____

City/State/Zip _____

Phone _____

Fax _____

E-mail _____

METHOD OF PAYMENT

❑ Check enclosed (to West Legalworks)

❑ BILL ME ❑ VISA ❑ MASTERCARD ❑ AMEX

Account # _____

Exp. Date _____

Signature _____

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