SUMMER 2000

First Amendment LAW LETTER

CONTENTS

Anonymity And The First Amendment: New Wrinkles In The Tension Between Anonymity and Accountablility

Busted! What To Do When Journalists Are Arrested On The Job

ICANN Uniform Domain-Name Dispute-Resolution Policy

ANONYMITY AND THE FIRST AMENDMENT: NEW WRINKLES IN THE TENSION BETWEEN ANONYMITY AND ACCOUNTABILITY

BY ANUJ DESAI

A dissident wants to send an e-mail with information aimed at exposing human rights abuses by her country's government. An unscrupulous "financial advisor" uses his website to manipulate the stock prices of individual companies by providing false information about alleged insider trading. A victim of sexual assault goes into a "chat room" to share her story with other victims. A hacker seeks to send an e-mail virus aimed at crippling computers world-wide. Each of these individuals has at least one thing in common. They all wish to remain anonymous.

Throughout history, anonymity has helped shield speakers of all kinds and has served both noble and nefarious goals. As technology makes communication easier, anonymity's power, to do both good and ill, likewise has increased. Moreover, while technology has in some ways reduced individuals' privacy by facilitating the sharing of information, recent technological advances - in particular, the use of powerful encryption - may lead to the day when anyone can communicate to a vast audience anonymously. These technologies will bring to the legal forefront the age-old dilemma of how to encourage and preserve anonymity for those with legitimate reasons while simultaneously ensuring the accountability necessary to enforce laws.

THE COSTS AND BENEFITS OF ANONYMITY

There are many valid reasons why one may wish to communicate without revealing one's identity, and society can benefit from permitting such communications.

CONTINUED ON PAGE 6

BUSTED! WHAT TO DO WHEN JOURNALISTS ARE ARRESTED ON THE JOB

BY SUSAN SEAGER AND JENNIFER BROCKETT

Pulitzer prize-winning Washington Post photographer Carol Guzy had never been arrested in her 20 years of work chronicling dangerous conflicts in Kosovo, Rwanda, or Haiti. But on April 15, 2000, Guzy was arrested in Washington, D.C. for allegedly "marching without a permit" while photographing demonstrations against the World Bank and International Monetary Fund. When she was released several hours later, "it was too late to use most of the film I'd shot that day," she lamented in a first-person account. Several days later, Los Angeles Times photographer Carolyn Cole was arrested in Miami while photographing skirmishes in the aftermath of the removal of Elian Gonzalez from the home of his relatives. A policeman claimed Cole threw rocks at him.

The Post's complaints about Guzy's arrest prompted police to drop the case against the photographer, but Cole's deliverance didn't come so easily. Her attorneys worked for several weeks to gather evidence and to persuade prosecutors that the arresting officer had confused Cole with a man who threw rocks at police, but who ran away when Cole tried to snap his photo and when police approached. "The more we looked into the charges, the more it was clear that a horrible mistake had been made," said John M. Hogan, a former prosecutor who represents media clients in civil and criminal matters in Florida. Prosecutors finally agreed not to pursue the case against Cole.

With civil disobedience back in vogue, media organizations and their lawyers are well advised to consider in advance how to respond if a working reporter or photographer is arrested. Media attorneys, who

CONTINUED ON NEXT PAGE

Davis Wright Tremaine LLP

BUSTED

CONTINUED FROM PREVIOUS PAGE

devote most of their practice to civil matters, can be caught off guard by the arrest of a journalist. History shows that reporters and photographers can be arrested anytime, even in covering routine news events, so it makes sense to have a general plan in place. Here are some tips from attorneys who have represented arrested reporters and photographers.

Have Criminal Defense Counsel Available. Civil media lawyers should have contacts with local criminal lawyers to respond to an arrest occurring during routine coverage. Moreover, when journalists are sent to distant locations - and particularly when civil unrest is anticipated - efforts should be made in advance to identify and contact criminal attorneys there. Karlene Goller, vice president and deputy general counsel for the Los Angeles Times, learned just how difficult it can be to find local criminal counsel in a distant city. Cole was arrested in Miami during Easter weekend, and most law offices were closed. "I was paged on a Saturday," recalls Goller. After many frantic calls, Goller finally found "the perfect guy": Hogan, a criminal and civil litigator with experience representing reporters and photographers. "It is critical to get a criminal defense lawyer who understands the First Amendment," Goller said. It also didn't hurt that Hogan was former chief of staff for Janet Reno, both when she was the Attorney General for the state of Florida and the United States, and that Hogan had hired the Miami prosecutors when he worked for the state attorney general's office.

Meet in Advance With Police. Schedule a meeting with police in advance of any event, such as the WTO meetings in Seattle or this summer's political conventions, that might result in arrests. Request attendance by a top member of the police brass with decision-making authority, not just the police department's media liaisons. "If I were going into this again, I would like to have someone's phone number with decision-making authority," said Eric Lieberman, associate counsel for the Post.

Guzy, her editors and the Post's in-house lawyers thought they had smartly avoided any trouble with police by scheduling face-to-face meetings with the police media liaison office in advance of the planned demonstrations last April. "Our advice to the photographers was to obey the police," Lieberman said. "We thought we had an understanding, but she got swept up in the mass arrest in the confusion that reigned that night." Guzy's editors could not reach her, nor could she call them while she was kept in custody for several hours in a school bus with demonstrators. Guzy said that she was released "earlier than most, with a little help from the Post." The "little help" was a telephone call by Mary Ann Werner, vice president and counsel for the Post. "Frankly, we called a top police official, who sent someone over to have her released," Lieberman said. "We didn't have any great legal solution. We just did some arm-twisting." The case against Guzy was not pursued. Police later declared her a "victim of circumstances," Guzy said.

Understand the Right to Criticize Police. Refusing to take no for an answer and pushing the limits to get the desired interview or the perfect shot can be hallmarks of good journalism. But newsgatherers should be advised to avoid antagonizing law enforcement officials who are poised to arrest them, or who are in the process of arresting them. "Tensions do run high. Cops feel they're losing control," said Melissa Widdifield, a Los Angeles criminal defense attorney who has represented three Los Angeles Times photographers arrested at separate events in recent years. A reporter or photographer who "mouths off" at an officer can trigger an arrest that otherwise might have been avoided. "That's who they go after - somebody whom they think is acting arrogantly, like they are above the law," Widdifield said.

Nevertheless, a reporter or photographer arrested simply for engaging in a verbal altercation with police might have grounds to challenge the arrest. In 1987, the United States Supreme Court struck down a Houston city ordinance that historically had been used to arrest reporters and individuals who argued with or criticized police. *City of Houston v. Hill,* 482 U.S. 451 (1987). The plaintiff, Raymond Wayne Hill, was arrested for yelling at police during their confrontation with a youth who was having a seizure. He was charged under an ordinance making it unlawful to "oppose, molest, abuse or interrupt any policeman in the execution of his duty." Hill challenged

The DWT Communications, Media and Information Technologies Department is experienced in the full range of legal issues facing the media, telecommunications, technology and related industries. Our attorneys assist broadcasters, publishers and journalists in all aspects of media law, including pre-publication review, access to courtrooms and public records, newsromm subpoenas and defamation, and invasion of privacy defense. We provide counseling, regulatory, business and litigation services for national and regional clients in the telecommunications, entertainment and computer industries and our First Amendment and intellectual property lawyers represent advertisers nationwide.

For more information on DWT's Communications, Media and Technologies Department, contact your DWT attorney at any of our offices below or call us on our toll-free client line at:

(877) 398 (DWT)-8415

Anchorage, AK
(907) 257-5300

Bellevue, WA
(425) 646-6100

Charlotte, NC
(704) 332-0800

Honolulu, HI
(808) 538-3360

Los Angeles, CA
(213) 633-6800

New York, NY
(212) 489-8230

Portland, OR
(503) 241-2300

San Francisco, CA
(415) 276-6500

Seattle, WA
(206) 622-3150

Washington, DC
(202) 508-6600

Shanghai, China
011-8621-6279-8560

or you can also email us at: **info@dwt.com**

the ordinance, and presented empirical evidence that police repeatedly used it to arrest those who criticized or argued with police, including reporters. The Court found that the law violated the First Amendment because it "criminalizes a substantial amount of constitutionally protected speech, and accords the police unconstitutional discretion in enforcement." *Id.* at 466. Justice Brennan, writing for the majority, declared that "the First Amendment protects a significant amount of verbal criticism and challenge directed at police officers" and that the "Constitution does not allow such speech to be made a crime." *Id.* at 461, 462.

First Amendment challenges to California's similar law, Penal Code Section 148, have failed in the state appellate courts, in part because the defendants were arrested strictly based on their conduct - such as running from a pursuing police officer - and because the defendants offered no empirical evidence that the police had used the law to arrest individuals solely based on their speech. *See In Re Andre P.,* 226 Cal. App. 3d 1164, 1175-79 (1991); *but see People v. Quiroga,* 16 Cal. App. 4th 961, 966 (1993) (defendant's refusal to disclose identity after arrest warranted conviction for violating Penal Code Section 148, but defendant theoretically would have "possessed the right under the First Amendment to dispute [the officer's] actions"). A challenge with better facts might have a better chance of success.

A reporter arrested for arguing with police may face a charge that his or her speech was combined with interfering conduct, or that the words themselves rise to the level of interfering with the officer. Indeed, a frequent charge against reporters and photographers is "disorderly conduct." In one New Jersey case, a photographer was convicted for disorderly conduct for refusing to step back from the scene of an accident and, allegedly, cursing at the police. The New Jersey Supreme Court held that the photographer committed disorderly conduct because he distracted the police officer on the scene for several minutes. A dissenting judge stated:

> The only "interference" caused [to the police officer] by defendant consisted of the alleged distraction deriving from defendant's photographing of the scene of the accident. In no other respect can it seriously be urged that the defendant as opposed to the non-media bystanders "obstructed" [the police officer] in the performance of his duties. Defendant's actions, however, constitute the precise type of conduct in which any media photographer must engage if he is to adequately report a news event. To characterize such conduct as an unreasonable interference with police activities is equivalent to a holding that the police may remove a newsman from the scene of an accident merely because that newsman is competently performing his job.

New Jersey v. Lashinksy, 81 N.J. 1, 20-21 (1979) (Pashman, J., dissenting). Nonetheless, in upholding the conviction, the majority noted that:

> [I]t has been recognized that the constitutional prerogatives of the press must yield, under appropriate circumstances, to other important and legitimate government interests. . . . The liberty which the press seeks to assure our people can be meaningfully employed only in a society where there is an adequate measure of order. . . . The Constitution does not serve to place the media or their representatives above the law. They are subject to law, as any citizen. The converse proposition would be intolerable. *Id.* at 13, 14.

As a practical matter, juries generally do not warm to people who are abusive toward police. The fact that Lawrence Erickson, a Redlands, California, photographer sentenced to six months in jail for allegedly "delaying" an officer at a crime scene in 1997, called officers "asshole" and "Buckwheat" did not help his lawyer paint him as a humble photojournalist just trying to do his job. Erickson argued that he was merely protesting the decision by police to bar him from taking photographs on a street that had been opened to traffic and pedestrians.

Finally, journalists who are arrested should take care to avoid any self-incriminating statements. Defense attorneys advise reporters and photographers to stop talking to the officer after being arrested, and to respond to

CONTINUED ON NEXT PAGE

BUSTED

CONTINUED FROM PREVIOUS PAGE

any attempt at questioning or conversation by stating that they have an attorney and will not speak to police or prosecutors until the attorney is present.

Understand the Right to Gather News. The Supreme Court has held that "newsgathering is not without its First Amendment protections," noting that "without some protection for seeking out the news, freedom of the press could be eviscerated." *Branzburg v. Hayes,* 408 U.S. 665, 681 (1972). Some states have recognized that "the right of the press to gather news is entitled to special constitutional protection," *Lashinsky,* 81 N.J. at 13, and other states have enacted legislation providing the press with a statutory right of access to disaster sites. *See, e.g.,* Cal. Penal Code § 409.5(d).

However, *Branzburg* also states that it "has generally been held that the First Amendment does not guarantee the press a constitutional right of special access to information not available to the public generally." *Branzburg,* 408 U.S. at 684. Based upon this dicta, several courts have upheld the convictions of reporters who followed demonstrators onto private or government property, or who refused to disperse when directed to do so by the police.

Sometimes, reporters who follow demonstrators onto private or government property or who are arrested as part of a sweep are not prosecuted, even when the state does prosecute the demonstrators. *See, e.g., Poullion v. City of Owosso*, 648 F.2d 1373 (1981) (of twenty-one people arrested for trespassing on government property, only the two reporters were not prosecuted). However, when reporters are prosecuted and convicted, courts have upheld those convictions, declaring that reporters are held to the same laws as everyone else. Reporters have been convicted of trespass for following demonstrators on to private property, and of disorderly conduct for refusing to obey police directions to step back. These convictions routinely are upheld on appeal.

For example, in *Stahl v. Oklahoma,* 665 P.2d 839 Okla. (1983), 339 demonstrators and nine reporters were convicted of trespass after being forbidden from demonstrating on the site of a proposed nuclear facility. In anticipation of the protest, the proposed site had confined reporters to a "public viewing area" inside the site. When the demonstrators left the area designated for demonstration, the nine reporters followed. In affirming the reporters' convictions, the majority held that

> the First Amendment does not guarantee the press a constitutional right of special access not available to the public generally. . . . [The reporters] were subjected to a rule of access applying to both press and public alike. This rule was supported by sufficient policy considerations.
> *Id.* at 842.

Other courts have reached the same result. For example, in *Oak Creek v. King,* 436 N.W.2d 285 (1989), the court upheld a reporter's conviction for disorderly conduct, where a reporter photographing an airline crash refused to leave a restricted area of an airport. The Wisconsin Supreme Court stated that "the appellant has an undoubted right to gather news from any source by means within the law. However, the appellant does not have a first amendment right of access, solely because he is a news gatherer, to the scene of this airplane crash when the general public has been reasonably excluded." *Id.* at 552. *But see City of Chicago v. Morales,* 527 U.S. 41, 62-63 (1999) (striking down loitering law as unconstitutional because it gave police too much discretion, failed to give adequate notice of forbidden conduct, and criminalized innocent behavior).

Carry Identification and Local Credentials. In addition to carrying press passes, members of the media should carry personal identification, such as a driver's license or passport, on their person. If possible, local press passes should be obtained. Cole, for example, had no local press credentials and no driver's license or passport when arrested, which made is difficult to persuade police that she was not a protester. The lack of identification also prolonged her booking, which took six to seven hours, Hogan said.

Sometimes, even local press credentials are of little help. Kery Murakami, a Seattle Post-Intelligencer reporter, said that he was slammed to the pavement by police and arrested for alleged failure to disperse while covering the World Trade Organization protests in Seattle last December. Police

Susan E. Seager, an associate in the Los Angeles office of Davis Wright Tremaine, worked as a newspaper and wire service reporter for more than a decade before becoming a lawyer. She represents journalists, publishers and broadcasters in libel, invasion of privacy and other content-related lawsuits, as well as in access matters.

Susan can be reached at (213) 633-6800 or susanseager@dwt.com

Jennifer L. Brockett, an associate in the Los Angeles office of Davis Wright Tremaine and a member of the Communications, Media and Information Technologies Practice Group, focuses her practice on First Amendment and intellectual property litigation, as well as advising clients regarding privacy issues.

Jennifer can be reached at (213) 633-6800 or jenniferbrockett@dwt.com

apparently took Murakami for one of many protesters who created their own press credentials and called themselves "the independent media." "I waved my press passes in front of my face," said Murakami, who, like police, was wearing a gas mask. "One of the cops yelled, 'So you think you can throw a bomb at us!'" Another officer said, "I can't trust what you are showing me because I've seen so many fake press passes." Murakami's editors called police when they noticed he was not telephoning them with updates on the demonstrations, and persuaded police to release him. No charges were filed.

Seek Post-Arrest Negotiation. Lawyers should move quickly to contact prosecutors and seek to avoid a trial. "It's all negotiation," Goller said. Widdifield recommends contacting the arresting officer as soon as possible. "Often after tempers have cooled, they often back down" from seeking formal charges, she said. Defense lawyers should ask to speak to the arresting officer, and to see any arrest reports as soon as possible. Often police claim that a reporter was interfering with their duties, but offer no evidence of the interference in their reports. Or, police and reporters jostle against each other, but there is no crime committed. "It's a rough-and-tumble world out there," Widdifield said. "Somebody's elbow could get in somebody's eye. But does it rise to the level of obstruction of justice?"

The case usually boils down to a battle of credibility, with police claiming that the reporter interfered with police, assaulted an officer, or obstructed justice. While defense lawyers say privately that they think officers sometimes exaggerate claims of reporter interference, it does no good to accuse the officers of trumping up charges. For example, Cole, the Los Angeles Times photographer arrested in Miami, had a tough time dissuading prosecutors that a police eyewitness had it all wrong. The arresting officer insisted that he saw her throwing rocks at police. "Our fear going in was he had sincerely believed he had seen her throwing rocks," Hogan said. As a former prosecutor, Hogan knows that prosecutors usually believe police over criminal suspects, and that he would gain nothing by attacking the officer as a liar. "Rather than attacking him, we said that he honestly believed that he saw Carol throwing rocks, but that he was mistaken." Hogan suggested that the officer's view was obscured by his gas mask and riot gear. Cole showed prosecutors all the photographs she had taken that day, although she had no photograph of the rock-thrower because he ran off when she attempted to take his picture. It took about a month of intense talks with police and prosecutors to persuade prosecutors to drop the case.

ANONYMITY

CONTINUED FROM PAGE 1

Recognizing some of these benefits, the United States Supreme Court in 1960 invalidated, on First Amendment overbreadth grounds, a Los Angeles ordinance that required all handbills to contain the author's name and address. *Talley v. California,* 362 U.S. 60 (1960). "It is plain," the Court observed, "that anonymity has sometimes been assumed for the most constructive purpose." *Id.* at 65.

One group of legitimate justifications falls broadly under the rubric of avoiding the stigma or group pressure associated with self-revelation. An on-line "chat room" for victims of sexual crimes is a good example of this. Being able to share intimate stories without disclosing one's identity makes it easier to express oneself fearlessly. Speaking anonymously, one can also take on different roles and/or hide one's physical attributes. No one has to know the speaker's race or gender, or whether one is physically disabled. The benefits of such identity-hiding have been documented by psychologists. *See* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces,* 104 YALE L.J. 1639, 1642 (1995).

In some circumstances, the stigma or group pressure associated with holding certain views or disclosing certain information can have serious repercussions, including reprisals. Potential whistleblowers may be fired and, in some countries, human rights activists risk jail - or worse - if their identity is discovered. In fact, those on the margins of society whose speech might threaten the status quo historically have needed the veil of anonymity for protection. As the Supreme Court noted in *Talley*, "[p]ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." *Talley,* 362 U.S. at 64.

A second way in which society benefits from preserving a right to communicate anonymously is the egalitarian goal of ensuring that ideas are judged by their content, not by the identity of their expositor. Social status is a powerful component in the persuasive power of certain ideas, and for those from the lower rungs of social stratification, being able to conceal one's identity can sometimes give one's ideas greater resonance and power.

But, permitting anonymity has costs as well as benefits, and the costs are based primarily on the very lack of accountability that makes anonymity attractive. One effect of anonymity is that readers or listeners will have reduced confidence in the accuracy of the information they receive, in much the same way that not knowing the origin of a consumer good (a car, a prescription drug, a can of soda) reduces confidence about it. Moreover, in some circumstances, the identity of the speaker is an important component of the content of the message. As the Supreme Court once noted, "An espousal of socialism may carry different implications when displayed on the grounds of a stately mansion than when posted on a factory wall or an ambulatory sandwich board." *City of Ladue v. Gilleo,* 512 U.S. 43, 56-57 (1994). By itself, though, this is hardly a reason to curtail anonymous speech. Readers and listeners can easily discount the value of such speech if they so choose.

The more important concern about anonymous speech is that it makes enforcing legitimate laws more difficult. A company seeking to determine who is divulging its trade secrets, an individual trying to determine who is defaming her, the government investigating the origins of an email-generated virus; all of these attempts to enforce necessary laws become extraordinarily difficult when one cannot easily determine the identity of the source. Related to the enforcement problem is the concomitant "moral-hazard" concern. By reducing the likelihood that wrong-doers will be detected, the possibility of anonymity may lead to an increase in harmful behavior. See David Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace,* 1996 U. CHI. LEGAL F. 139, 142.

ANONYMITY IN CYBERSPACE

New and interesting legal issues that highlight the tension between anonymity and accountability have come to the fore in cyberspace. To participate in most on-line "chat rooms," for example, all one needs is a "screen name," and the screen name need not reveal one's true identity. This has led to problems with many chat rooms including, for example, those devoted to specific publicly-traded companies: An anonymous participant will make a derogatory comment about the

Anuj Desai, an associate in the Seattle office of DWT, focuses his practice on Internet, First Amendment and Intellectual Property Law. His experience includes First Amendment, defamation, newsgathering, copyright and trademark litigation (both trial and appellate level); drafting co-linking and co-marketing Internet agreements; and advising clients with respect to First Amendment, copyright and privacy issues.

Anuj can be reached at (206) 628-7714 or anujdesai@dwt.com

company or its management, and the company will take offense. The company may respond by bringing suit against an unnamed party - which is possible in most states simply by naming "John Doe" as a defendant - and then obtaining subpoenas against the chat-room provider or other entity that might have information about the true identity of the anonymous poster.

According to some commentators, the ease with which a subpoena may be obtained has led some companies to use the tactic to silence critics and chill free speech even when they do not have a legitimate claim against the putative defendant. Consider the example of Raytheon, a Massachusetts-based defense contractor. It suspected that some employees were divulging company secrets on a Yahoo! site and brought suit against 21 "John Does." It then served subpoenas on Yahoo! and eventually learned all 21 names. Yet as soon as it discovered the identities of its defendants, it dropped the suit, leading David Sobel, general counsel for the Electronic Privacy Information Center (EPIC), a privacy watchdog group, to accuse Raytheon of misusing the subpoena power: "It seems that the sole objective of Raytheon was to identify those individuals," Sobel said. *Raytheon Drops Suite Over Internet Chat, N.Y. Times,* May 22, 1999.

Or, consider Itex, an online bartering company that brought suit against a John Doe who turned out to be a former executive, Les French. When French decided to continue the fight after being unmasked, Itex lost its appetite for litigation. Itex ended up paying French $45,000 in the resulting settlement (of which $40,000 went to an organization that French set up to help cyberspeech defendants, the John Does Anonymous Foundation, <www.johndoes.org>), in exchange simply for a promise by French not to file a countersuit for malicious prosecution.

Despite the fact that providers of interactive online services are immune from liability in most circumstances, 47 U.S.C. § 230(c), the Raytheon and Itex examples illustrate one important issue facing chat-room hosts. On the one hand, they want to maintain lively sites that encourage a wide range of comments, both good and bad, about companies; to do that, anonymity is a valuable tool. Yet, at the same time, they do not want to get involved in every legal battle involving statements made on their sites. What most online hosts have done is to include in their Terms of Service agreement a provision that permits disclosure of the user's identity if the host has a good-faith belief that such disclosure is required by law. Though one chat room participant has brought suit against Yahoo! for disclosing his identity, courts will likely consider the receipt of a subpoena to be sufficient grounds for a good faith belief that the law required disclosure. See John Doe Fights Back by Suing Yahoo! for Privacy Infringement, <http://www.epic.org/privacy/anonymity/aquacool-release.html>.

Many hosts have also instituted a policy of providing notice to the chat-room participant before disclosing any information in response to a subpoena, so as to give the user the opportunity to quash the subpoena. As long as courts are willing to quash subpoenas in meritless suits, this may be an appropriate solution, since it allows cyberspeech defendants to try to protect their own identity. If John Doe can preclude the unmasking of his identity until after a court rules on a motion to dismiss, this may be the fairest way to balance John Doe's right to remain anonymous with a plaintiff's right to prosecute a legitimate lawsuit. This approach, however, likely will raise interesting questions about service of process and jurisdiction.

NEW TECHNOLOGIES AND ANONYMITY

The risk of cyberspeech lawsuits may lead those seeking anonymity to look for new technologies to help cloak their identity. Several companies recently have begun offering sophisticated methods for preserving anonymity using encryption. A Canadian company, Zero-Knowledge, has introduced a software program called "Freedom 1.0" that combines three separate components - "nyms," encryption and what the company calls its "Freedom Network." "Nyms" are pseudonyms a person chooses. Once the software program is activated, it automatically encrypts all of a customer's Internet traffic within multiple layers of cryptography. The "Freedom Network," which is a group of servers Zero-Knowledge maintains, then further encrypts the data so that the only information left is the chosen "nym." Zero-Knowledge claims that its system even strips out all information about a user's ISP and that the most one can recover from their servers is an encrypted stream of data. The company also claims that, although it does collect a credit card number

CONTINUED ON NEXT PAGE

ANONYMITY

CONTINUED FROM PREVIOUS PAGE

before letting you download its software, it cannot link the credit card number to any particular nym. See Patrick Norton, Freedom 1.0., ZDNet/PC Magazine (Dec. 23, 1999), <http://www.zdnet.com/pcmag/stories/first-looks/0,6763,2413285,00.html>. So, Zero-Knowledge claims that, even if issued a subpoena, it would not have any information to give.

Another new system of maintaining anonymity online was recently unveiled by researchers at AT&T Labs. Named "Publius," after the pseudonym used by Alexander Hamilton, John Jay and James Madison to publish the Federalist Papers, the AT&T system also uses sophisticated encryption and has the additional advantage of being hosted by a system of volunteer servers throughout the world. The result, say the system's developers, is that there is no central repository of the information necessary to track an author.

Whether any of the attempts to create perfect anonymity succeeds remains to be seen. In the meantime, society and the courts will continue to have to grapple with the important question of how to protect legitimate anonymity while ensuring that the legal system can expose those who use the cover of anonymity to break laws.

ICANN UNIFORM DOMAIN-NAME DISPUTE-RESOLUTION POLICY

BY ALEXANDRA NICHOLSON, ANUJ DESAI, JEFFREY H. BLUM AND MATTHEW A. LEISH

Internet domain names are valuable property, so it is unsurprising that disputes about them are becoming more common. The Internet Corporation for Assigned Names and Numbers ("ICANN"), the nonprofit organization currently overseeing many Internet management functions, has created a new streamlined procedure for resolving disputes about domain names within the .com, .net and .org top-level domains. The procedure is embodied in the Uniform Domain-Name Dispute-Resolution Policy ("UDRP" or "Policy"), which became effective on December 1, 1999.

The UDRP provides an inexpensive and efficient way to resolve domain-name disputes. Generally, decisions are made within five weeks of the filing of a complaint. The arbitration panel's fees are relatively modest - from $750 to $3,750, depending upon the number of domain names in dispute and the number of arbitrators the complainant requests - and because each side generally submits only one document (a pleading/brief combination), the legal fees are also generally lower than a court case.

Given the ease, low cost and speed of the process, it is not surprising that a wide variety of parties have already brought cases under the Policy. Complainants include major corporations such as Microsoft and Hewlett-Packard, individuals such as actor Brad Pitt and singer/songwriter Peter Gabriel, and educational and non-profit institutions such as Oxford University and Emory Hospital. As of August 14, 2000, over 1,400 cases involving more than 2,500 different domain names had been commenced. The procedures permit complainants to choose among a list of arbitration providers approved by ICANN. As of August 2000, there are four approved providers: the World Intellectual Property Organization (WIPO), the National Arbitration Forum (NAF), Disputes.org/eResolution Consortium (DeC), and CPR Institute for Dispute Resolution.[1]

One key limitation on the Policy is that the only remedy the arbitrator(s) can order is a transfer or cancellation of the domain name registration. Other remedies, such as money damages, are not available. Moreover, the Policy permits either party to submit the dispute to a court for independent resolution before or after the mandatory administrative hearing is concluded. So, in the United States, a complainant who wanted damages would bring a civil suit under the new Anti-cybersquatting Consumer Protection Act.[2] At this point, it remains an open question whether a losing party can relitigate issues decided by a UDRP arbitral panel, and, if so, how much deference courts will give panel decisions.[3]

Under the Policy, a complainant must prove three things to obtain a transfer of a domain name:

(1) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
(2) the registrant has no rights or legitimate interests with respect to the domain name; and
(3) the domain name has been registered and is being used in "bad faith."

The first requirement is a change from the pre-UDRP dispute-resolution policy administered by Network Solutions, the company that was initially the sole registrar of .com, .net, and .org domain names. Under the Network Solutions policy, the domain name had to be identical to the complainant's trademark or service mark. This precluded recovery against cybersquatters who had used punctuation or spelling variations to register domain names that were only slightly different from pre-existing trademarks. Under the UDRP, however, a "confusingly similar" domain name is enough. So, for example, General Electric brought a complaint and eventually prevailed against the registrant of general-electric.com.[4]

A registrant can preclude the complainant from proving the second requirement by showing that it has "rights or legitimate interests" in the domain name. It can do this in one of several ways:

(a) by using the domain name in connection with a bona fide offering of goods or services before having notice of the complaint;
(b) by being commonly known by the domain name (whether or not this rises to the level of trademark or service mark rights); or
(c) by making legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark of another.

As for the third requirement - "bad faith" on the part of the registrant - there are many ways the complainant can show this. For example, the complaining trademark owner may show that the registrant intended to sell the domain name to the complainant, to direct traffic to the registrant's site for commercial gain, or to otherwise create a likelihood of confusion as to the source, sponsorship, affiliation or endorsement of the registrant's web site. Or, the complainant can show that the registrant is a competitor trying to disrupt its business. As explained below, this "bad faith" requirement has generated much of the interesting debate about cases brought under the UDRP.

An example of a recent, successful ICANN complaint is the one brought by Guccione Media, LLC, the owner of Gear magazine.[5] The complaint alleged that Charles Duncan and his company, CTC Entertainment, had registered the domain name "GEARMAGAZINE.COM" and created a "website preview" on the site consisting of photographs and text taken directly from Gear without authorization. Duncan had then written to Gear proposing, in essence, that Gear either purchase the website from him or hire him to run the website on Gear's behalf. After Guccione Media contacted Duncan and demanded that he promptly remove all content related to Gear from the website and transfer the domain name to Guccione Media, Duncan responded that his actions had been "misinterpreted," and he agreed to transfer the name - provided that Gear "reimburse [his] investment costs" of approximately $2,000. When Gear declined to pay the "investment costs," Duncan then changed his story, asserting in a subsequent letter that the web site "has nothing to do with Gear magazine" and making it clear that he intended to

CONTINUED ON NEXT PAGE

ICANN

CONTINUED FROM PREVIOUS PAGE

retain ownership of the domain name.

Pursuant to the ICANN Policy and Rules, Guccione Media filed its complaint on April 11, 2000. Approximately four weeks later, the arbitrator ruled in Guccione Media's favor, finding that Duncan had "no rights or legitimate interests" in the domain name, and that the domain name had been "registered and [was] being used in bad faith." Accordingly, the arbitrator ordered that the domain name be transferred to Guccione Media. Under the ICANN rules, Duncan had ten days to file a federal lawsuit to stop the domain name transfer. He did not do so, and Network Solutions proceeded to transfer the domain name.

The Gear Magazine case is hardly unique, and trademark holders have been successful in ousting cybersquatters in many other cases. For example, the World Wrestling Federation successfully wrested worldwrestlingfederation.com from a cybersquatter in the very first case decided under the Policy. [6] Julia Roberts won juliaroberts.com from a fan, who responded to the complaint by stating that, "If Julia Roberts had picked up a phone and said, 'Hi Russ, Can we talk about the domain name juliaroberts.com?' she would own it by now."[7] These cases, like the Gear Magazine case, present some of the easier cases for panels.

Some commentators have argued, though, that the ICANN panels have unfairly favored trademark holders.[8] For example, in one recent case, Hearst Publications, the owner of Esquire Magazine and numerous trademark registrations for the word "Esquire," brought a complaint against the owner of esquire.com. Based on Hearst's trademark registrations and the fact that the word "Esquire" is widely associated with the magazine in many people's minds, the panel ordered esquire.com transferred to Hearst.[9] Yet, the person who originally registered it did so in 1994, years before anyone had even heard of cybersquatting as an offense, and he did so thinking of the word "esquire" as the lawyers' courtesy title. The only "bad faith" that the panel found was that the registrant had a business selling domain names and tried to sell esquire.com. Yet, there was no evidence he had ever tried to sell it to Hearst, and he was in fact under contract to sell it to mail.com, a company that provides "vanity" e-mail services through domain names like accountant.com, doctor.com and lawyer.com.

Another questionable decision involved the transfer of crew.com to the retail clothing store, J. Crew.[10] As with the esquire.com case, the "bad faith" found in the crew.com case was based on the fact that the registrant had made the domain name available for sale. Criticism of the panel's decision was likewise based on the fact that "crew" is an ordinary word found in the dictionary and there was no evidence that the registrant specifically aimed the sale at the complainant trademark holder.

In another criticized case, a Canadian company called eResolution.ca (one of the UDRP's approved dispute-resolution service providers) sought the domain name eresolution.com. The panel ordered the name be transferred despite the fact that the registrant had obtained the domain name several months before eResolution.ca had even come into existence and thus before having any reason to know that anyone had trademark rights in "eresolution."[11]

While trademark holders have prevailed in the great majority of circumstances, there are exceptions. Some panels have effectively disagreed with the esquire.com and crew.com decisions by holding that the mere offering of a domain name broadly for sale to the public is not "bad faith" when the registrant is unaware of the trademark holder's rights. Panels can easily find a lack of bad faith when the trademark holder's rights are based on an arbitrary or descriptive mark. So, for example, General Machine Products Company, Inc., the owner of a trademark in "craftwork," was unable to obtain a transfer of the domain name craftwork.com from a respondent whose business was selling domain names.[12] In another case, the Western Hay Company sought the domain names westernhay.com and westernhay.net from the spouse of a former jockey who was using the site as a discussion group to educate people on how to care for horses, including the nutritive merits of feeding them western hay. The panel refused to find evidence of "bad faith" because, when approached by Western Hay Company to sell the domain name, the registrant asked only for the costs of registration plus an apology to his wife, a former customer of Western Hay Company, who had allegedly been verbally mistreated by one of the

Alexandra Nicholson, a partner in DWT's New York office, represents a wide range of clients on intellectual property matters. She regularly advises clients on trademark and domain name issues and is a frequent writer and speaker on these subjects. She represented Gear Magazine in the ICANN dispute described in this article.

Allie can be reached at (212) 489-8230 or allienicholson@dwt.com

Jeffrey H. Blum is an associate in Davis Wright Tremaine's New York City Office. His practice is focused on general communications and media issues, with specific emphasis on First Amendment litigation and Internet issues.

He has co-authored the New York section of the Libel Defense Resource Center, 50-State Survey (Media Privacy and Related Law) and is the co-author of "Online Service Provider Liability Under the Digital Millennium Copyright Act," Communications Lawyer, Vol. 17 (Fall 1999). Mr. Blum represented Gear Magazine in the ICANN dispute described in this article.

Jeff can be reached at (212) 489-8230 or jeffblum@dwt.com.

Matthew A. Leish is an associate in DWT's New York City office. His practice is focused on communications and media law, with specific emphasis on First Amendment litigation issues.

Matt can be reached at (212) 603-6410 or mattleish@dwt.com

company's employees.[13] These cases suggest that, in general, it will be more difficult for those whose trademarks are arbitrary or descriptive to prevail because of the wide range of uses for many ordinary words.

Finally, in a case of some note because of the worldwide trademark registrations and significant international presence of the complainant, the Japanese photo film company, Fuji Photo Film Co Ltd., and its U.S. subsidiary sought the domain name fuji.com from a Tacoma, Washington business software and web design company, Fuji Publishing Group LLC. Holding that Fuji Publishing had both rights and a legitimate interest in the fuji.com domain name because it was a legitimate business offering goods and services different from those of Fuji Film, the panel refused to order the transfer of the name.[14]

In sum, the new ICANN Uniform Dispute-Resolution Policy has already made a significant contribution towards the fast and efficient resolution of domain-name disputes. As with any new process, there will be growing pains and important questions, not only about the substance of the decisions made by the arbitrators but also about the intersection of UDRP proceedings, which involve only the possibility of domain-name transfers and are limited to applying the UDRP's three-pronged standard, and U.S. courts that must apply the Anti-Cybersquatting Consumer Protection Act and have the full panoply of remedies. But the relatively modest cost of the proceedings and the speed with which decisions are made suggest that more parties will seek relief under the UDRP despite the Policy's limitation.

[1]The list of approved providers can be found at <www.icann.org/udrp/approved-providers.htm>.

[2]*See* 15 U.S.C. § 1125(d) (2000); *see also* Marshall J. Nelson, *Cybersquatting or Cyberspeech: First Amendment Issues in the New Anticybersquatting Act*, FIRST AMEND. L. LETTER (Winter 2000) http://www.dwt.com/related_links/adv_bulletins/CMITWint2000LawLetter.htm#b2

[3]*See Weber-Stephen v. Armitage*, Mem. Op. and Order at 4 (No. 00 C 1738: N.D. Ill. May 3, 2000) (Aspen J.), http://www.ilnd.uscourts.gov/JUDGE/ASPEN/MEA_OPIN/00C1738.pdf (holding that U.S. courts are not bound by UDRP administrative proceedings, but leaving open the question of how much weight to give the panel's decision).

[4]*General Electric Co. v. Bahkit,* Case No. D2000-0386 (WIPO June 22, 2000) http://www.arbiter.wipo.int/domains/decisions/ html/d2000-0386.html

[5]Davis Wright Tremaine LLP represented Guccione Media in the ICANN proceeding.

[6]*World Wrestling Fed'n Entertainment v. Bosman,* Case No. D99-0001 (WIPO Jan. 14, 2000), http://arbiter.wipo.int/domains/decisions/html/d99-0001.html. Decisions under the UDRP can be found through ICANN's website, http://www.icann.org/udrp/udrp.htm.

[7]*Roberts v. Boyd,* Case No. D2000-0210 (WIPO May 29, 2000), http://arbiter.wipo.int/domains/decisions/html/d2000-0210.html.

[8]*See, e.g.,* Michael Geist, Domain Name Wars Heat Up, THE GLOBE & MAIL, May 4, 2000, http://www.globetechnology.com/archive/gam/E-Business/20000504/TWGEIS.html.

[9]*Hearst Communications, Inc. v. Spencer,* Case No. FA0093763 (NAF Apr. 13, 2000), http://www.arbforum.com/domains/decisions/93763.htm.

[10]*J. Crew Int'l Inc. v. crew.com,* Case No. D2000-0054 (WIPO Apr. 20, 2000), http://arbiter.wipo.int/domains/decisions/html/d2000-0054.html.

[11]3636275 Canada v. eResolution.com, Case No. D2000-0110 (WIPO Apr. 10, 2000), http://arbiter.wipo.int/domains/decisions/html/d2000-0110.html.

[12]*General Machine Prods. Co. v. Prime Domains,* Case No. FA0092531 (NAF Commenced on Jan. 26, 2000), http://www.arbforum.com/domains/decisions/ 92531.html

[13]*Western Hay Co. v. Forester,* Case No. FA0093436 (NAF Mar. 3, 2000), http://www.arbforum.com/domains/decisions/93466.html.

[14]*Fuji Photo Film Co. v. Fuji Publ'g Group,* Case No. D2000-0409 (WIPO July 2, 2000), http://arbiter.wipo.int/domains/decisions/html/d2000-0409.html.

This *First Amendment Law Letter* is a publication of the law firm of Davis Wright Tremaine LLP and is prepared by its Communications, Media and Information Technologies Department, P. Cameron DeVore, Chair, Eric Stahl, Editor, and Alonzo Wickers IV, Associate Editor. Our purpose in publishing this law letter is to inform our clients and friends of recent First Amendment developments. It is not intended, nor should it be used, as a substitute for specific legal advice since legal counsel may be given only in response to inquiries regarding particular factual situations.

To change your address, to request electronic delivery of this publication, or to receive additional information, please contact Sandy Andolora in our Seattle, Washington office at (206) 628-7448 or sandyandolora@dwt.com.

Printed on Recycled Paper

Davis Wright Tremaine LLP
2600 Century Square
1501 Fourth Avenue
Seattle, Washington 98101-1688

**FIRST CLASS
PRE-SORT
U.S POSTAGE PAID
SEATTLE, WA
PERMIT NO. 1538**

www.dwt.com

Davis Wright Tremaine LLP