

eDiscovery

Technology and Law

A Special Supplement To The Connecticut Law Tribune

ALM

Avatar Law Firms Take To Cyberspace

Second Life's legal disputes
are fertile ground for
tech-savvy lawyers

P.5



inside

Computer Forensics:
Discover the smoking gun in e-discovery p.2

The New Rule 26:
Needle in a haystack of e-documents p.3

SECURITY BREACH

Secrets Of The Computer Hard Drive

How computer forensics can help you find the smoking gun in electronic discovery

By **BRIAN C. ROCHE**
and **GERALD C. PIA, JR.**

With the enactment of the 2006 amendments to the Federal Rules of Civil Procedure, litigators are now trying to wrestle with the many significant revisions affecting the discovery of electronic data. While the potential breadth of the rules can seem daunting, some lawyers have become focused on how they can best extract the “smoking gun” from an adversary’s electronic materials. But finding the “smoking gun” often starts with an early forensic search of your client’s own computers.

Consider the following case study: You represent a company whose primary asset is its intellec-

tual property and trade secret material. The company has advised you that one of its key employees has recently left his position and is now working for a direct competitor. Several of the company’s best customers have reported that they were recently contacted by this employee, who has offered to beat your client’s special pricing arrangements on numerous products. The customers naturally expect your client to adjust its prices accordingly in order to continue their business relationship. Based on these facts, it appears that this employee took more than his favorite coffee mug when he left the company—namely, the company’s proprietary information and trade secrets.

As a counselor, you need to advise your client on the preliminary steps that it should take as a result of this employee’s departure. Obviously, the client needs to conduct an investigation to develop additional facts related to the former employee’s misconduct. One primary component of that investigation should be a forensic investigation—that is, an analysis of the former employee’s desktop and laptop computers utilized during the course of the individual’s employment with the company.

mine (1) what exactly happened, and (2) who is responsible for the conduct at issue. Whether your client chooses to utilize an outside firm capable of performing these services or an internal IT/security officer, any examination must be performed with eye towards recovering and preserving the integrity of the original data located on the computer or device, and ultimately presenting testimony that will withstand cross-examination.

Many of us now recognize that an individual cannot simply delete information from his computer and expect to permanently remove any trace that it ever existed. Most data that are written to a hard drive or similar media will remain there until they are actually overwritten by additional/new

data. Until the “deleted” data are overwritten they will continue to reside on the hard drive; only the “link” to that data is removed. A useful analogy is to consider the classic card catalog system utilized in your elementary school library when you were a student. If one removed an index card from the card catalog, it did not mean that the book referenced on that card ceased to exist. Only the “link” was removed. One capable of navigating his or her way through the library could still locate the book from the library shelves, unless that book was actually removed from the library and replaced with a new volume.

The benefits of an early forensic analysis can be significant. A successful examination can greatly impact the likelihood of your client’s success at a preliminary injunction hearing, alter the tenor of settlement negotiations, or justify a (sometimes intrusive) forensic analysis of a defendant’s (or even a third party’s) computer system.

Consider the following hypothetical similar to our case study. The departing employee, who had entered into a non-compete and confidentiality agreement with our client, and who indicated that he would be leaving the industry, becomes employed immediately by our client’s direct competitor. The defendant took unreasonable positions during the parties’ preliminary settlement discussions, suggesting that our client could never prove wrongdoing. Moreover, after receiving a motion for expedited discovery in connection with a preliminary injunction hearing, the defendant’s counsel responded orally that our pursuit was wasteful because “no responsive documents existed.”

Unbeknownst to the defendant at the time, our client had wisely decided to perform an early forensic analysis to assess the employee’s pre-resignation conduct. The results provided us with early signs of the proverbial “smoking gun,” as well as proof that other information – perhaps *the* “smoking gun” existed on the defendant’s and/or his new employer’s computers. The analysis revealed that the former employee had been negotiating for months with his new employer over the specifics of his new opportunity, while still employed with the company. It further demonstrated, through recovered e-mails, that the former employee had gone so far as to divert business opportunities to his potential new employer in an apparent effort to curry favor. Finally, the analysis demonstrated that the employee had connected a USB “flash drive” to his work computer and downloaded suspicious files (which he had attempted to rename and/or delete), in the format in which our client’s confidential trade secrets are kept. There was little doubt that the defendant had copied this information to his and/or his new employer’s computers, and that electronic discovery would reveal this.

Deflating The Defense

Armed with the results of the forensic examination, we were able to deflate the defendant’s “good guy” defense, warn the defendant that we would seek examinations of the defendant’s and his new employer’s computers and media, and significantly alter the tenor of the settlement negotiations that had begun. Presented with a “taste” of the information recovered during the forensic analysis, the defendant’s counsel became better able to advise his client – and his client’s new employer (whom the attorney also represented) – on the risks posed by the litigation, as well as opine on the extent of the parties’ exposure.

Suffice it to say, this case did not proceed to trial. Indeed, it settled before the anticipated electronic discovery was formally commenced. The defendant’s counsel—like most litigators—was well aware of the potential scope of electronic discovery under the 2006 amendments, especially where, as here, the data recovered by our client would justify an examination of both the defendant’s and his new employer’s computer systems. Because our client’s demands had been reasonable, the end result was a quick and favorable resolution for our client. The moral of the story? The “smoking gun”—or at least a map to it—may be buried within your client’s own computers. Start there. ■



There was little doubt that the defendant had copied [our client's trade secrets] to his and/or his new employer's computers, and that electronic discovery would reveal this.



tual property and trade secret material. The company has advised you that one of its key employees has recently left his position and is now working for a direct competitor. Several of the company’s best customers have reported that they were recently contacted by this employee, who has offered to beat your client’s special pricing arrangements on numerous products. The customers naturally expect your client to adjust its prices accordingly in order to continue their business relationship. Based on these facts, it appears that this employee took more than his favorite coffee mug when he left the company—namely, the company’s proprietary information and trade secrets.

As a counselor, you need to advise your client on the preliminary steps that it should take as a result of this employee’s departure. Obviously, the client needs to conduct an investigation to develop additional facts related to the former employee’s misconduct. One primary component of that investigation should be a forensic investigation—that is, an analysis of the former employee’s desktop and laptop computers utilized during the course of the individual’s employment with the company.

Finding The Trail

Computer forensics can generally be defined as the analysis of digital media after a computer security issue has arisen. The goal of this analysis is to deter-

Brian C. Roche and Gerald C. Pia, Jr. are partners in the law firm of Roche Pia LLC in Shelton.

mining the defendant’s computer system. Consider the following hypothetical similar to our case study. The departing employee, who had entered into a non-compete and confidentiality agreement with our client, and who indicated that he would be leaving the industry, becomes employed immediately by our client’s direct competitor.

The benefits of an early forensic analysis can be significant. A successful examination can greatly impact the likelihood of your client’s success at a preliminary injunction hearing, alter the tenor of settlement negotiations, or justify a (sometimes intrusive) forensic analysis of a defendant’s (or even a third party’s) computer system.

Consider the following hypothetical similar to our case study. The departing employee, who had entered into a non-compete and confidentiality agreement with our client, and who indicated that he would be leaving the industry, becomes employed immediately by our client’s direct competitor.

Tell-Tale Signs

After we commenced litigation, the former employee’s attorney consistently repeated the mantra that “the defendant was a good guy” and accused our client of being the “school-yard bully.” Apparently hoping to hide behind this line of defense, the defen-

DISCOVERY DISASTER

New Rules Help Deal With Inadvertent Disclosure

Procedures for claiming privilege include giving disputed document to the court under seal

By **BRADFORD BABBITT**
and **BRETT BOSKIEWICZ**

The inadvertent disclosure of privileged documents has been a risk for clients and a worry for lawyers since the dawn of document discovery. Clients incur untold expense in document review attempting to avoid a mistake that could reveal their communications with counsel. Lawyers spend sleepless nights worrying that there may be a privileged needle hiding in the haystack of production. The Federal Rules of Civil Procedure were, until recently, silent on this issue. Although silent no longer, what they have to say doesn't

asserted. Under the new rule, parties who learn that documents that they claim are the subject of a privilege have been produced must notify the receiving party of the claim and the basis for it. After being notified, the receiving party must promptly return, sequester, or destroy the document and any copies of it and may not use or disclose the document until the claim is resolved. The party that received the document may, instead, promptly present the document to the court under seal for a determination of whether the document is privileged and whether the privilege has been waived. If the receiving party disclosed the documents to others before learning that the producing party claimed it was privileged, the

intentionally or accidentally. Some courts even deem the inadvertent disclosure of one document to waive the privilege as to "all other communications relating to the same subject matter." Both the strict and lenient approaches apply only in a minority of jurisdictions. See *Gray v. Bicknell*, 86 F.3d 1472, 1483 (8th Cir. 1996) (discussing the three approaches).

Most courts, including both state and federal courts in Connecticut, apply the "middle of the road" approach and strike a balance by not punishing a reasonably cautious party for an accidental disclosure and by not rewarding a party's cavalier approach to confidentiality. See e.g., *Harp v. King*, 266 Conn. 747 (2003); *Travel Insured Int'l, Inc., v. iTravelInsured, Inc.*, No. 3:05cv1305, 2005 U.S. Dist. LEXIS 41881, at 3-4 (D. Conn. November 28, 2005) (citing cases applying middle of road approach).

Courts strike this balance by considering five factors to determine whether the inadvertent disclosure constituted a waiver of the privilege. These factors are:

- precautions taken to avoid inadvertent disclosure;
- number of times documents were inadvertently disclosed;
- number of documents inadvertently disclosed;
- speed with which the client acted to correct the disclosure; and
- overriding interest of justice.

Balancing these factors

requires a detailed inquiry into the document practices of the party who inadvertently released the document. To maintain the privilege, the disclosing party must show that it took reasonable steps to maintain its confidentiality and that the document was nonetheless accidentally disclosed. The number of documents produced overall factors into the analysis of whether the client took reasonable precautions. Courts consider the number of times documents were inadvertently disclosed and the number of documents disclosed as part of the evaluation of whether the client acted reasonably. Courts applying the "middle of the road" approach recognize that "reasonable precautions are not necessarily foolproof." *Harp*, 266 Conn. at 773.

In sum, the new amendments to Rule 16 and 26 encourage the parties to discuss and to adopt an agreement governing the assertion of privilege with respect to documents that have already been produced. Even in the absence of such an agreement, however, Rule 26 now provides a mechanism for stopping the spread of potentially privileged documents before the claim can be resolved by the court. The new rules will not, however, change the way courts resolve disputes over the privilege status of a document that has already been produced. In Connecticut, that will continue to depend on the multiple factors that make up the "middle of the road" approach. These rule amendments, while certainly not eliminating the cost of document review or ensuring a full night's sleep for counsel, are a step in the right direction. ■



Rule 26 now provides a mechanism for stopping the spread of potentially privileged documents before the claim can be resolved by the court.



much change the landscape for clients or their counsel.

The New Federal Rules

Amendments to the Federal Rules of Civil Procedure adopted in December 2006 included three changes directly addressed to the issue of the inadvertent disclosure of privileged documents. The first appears in Rule 16, which governs scheduling conferences and orders. Rule 16(b) has been amended to include among the topics to be addressed in a scheduling order any agreements the parties may have reached for asserting claims of privilege with respect to documents already produced.

A second change appears in Rule 26(f) and is a corollary to the Rule 16(b) change. Since the amendments, Rule 26(f) now obliges the parties to discuss, in their pre-discovery conference, whether they agree to a procedure for asserting privilege after a document had been produced and whether they want the court to enter that agreement as an order.

Rule 26 also incorporates the third and most substantial change related to the inadvertent disclosure issue. Rule 26(b)(5)(B) has been amended to create a standard procedure for handling documents that have been produced before a claim of privilege is

receiving party must take reasonable steps to retrieve the document. The producing party is obliged to preserve the document until the court resolves the claim.

The new text of Rule 26 codifies many of the procedures used in typical "clawback agreements" among litigants. Even in the absence of a specific agreement among the parties governing inadvertent disclosure, Rule 26 stops the spread of potentially privileged documents until the claim of privilege is resolved. The new amendments also creates a mechanism by which the claim can be resolved quickly by permitting receiving parties to submit the disputed document to the court under seal instead of returning the document to the producing party.

None of the newly amended federal rules address the resolution of a disputed claim of privilege with respect to a document that has already been produced. That analysis, which varies by jurisdiction, remains unchanged by the amendments to Rule 16 and 26.

Analysis of Post-Production Privilege

Courts have adopted three different approaches in considering whether inadvertent disclosure waived the attorney-client privilege. The "lenient approach" maintains the privilege if a party demonstrates that the disclosure was truly inadvertent. The rationale for this view is that only an intentional act can waive the attorney-client privilege. The "strict approach" is, not surprisingly, just the opposite: any disclosed document loses its privilege regardless of whether the party produced it

Bradford Babbitt is a partner in Robinson & Cole's Trial and Appellate section and chair of the Business Litigation practice group. Brett Boskiewicz is an associate in the firm's Trial and Appellate and Labor, Employment, and Benefits sections.

COMPUTER CRIME

Cyberinsurance: An Added Layer of Security

Many law firms inadequately protected from online breach

By EDWARD POLL

Confidential client records and work product are the core of any law firm's work product. Most firms understand the necessity of archiving computer and paper files in a safe, off-site location. But what about the active files on your computer?

If they are compromised by a hacker, or otherwise threatened by criminal activity, how would it affect your operation?

A recent survey of businesses and professional organizations, conducted jointly by the Federal Bureau of Investigation and the Computer Security Institute, provides these chilling statistics:



Failure to reasonably anticipate and be prepared to service clients in the wake of a disaster is arguably a failure in the overall duty to act competently.

Ninety percent of survey participants have suffered a computer security breach, with average losses running into the hundreds of thousands of dollars.

The two biggest sources of financial loss from computer security breaches are viruses (accounting for 33 percent of the total) and unauthorized access (causing one-fourth of all computer security losses).

Theft of proprietary information is the fastest rising cause of computer security financial loss, doubling from the year before in the most recent survey.

Liability Insurance

Most firms have some form of liability insurance to protect premises and their contents against losses from fire or other disasters. But computer security risks are fundamentally different—and fundamentally unprotected by most policies.

Several years ago, Ernst & Young surveyed several thousand organizations about whether they had insurance coverage for losses related to computer security. More than 33 percent of respon-

dents thought they had coverage through their general liability policies, but in fact did not. More than half either knew that they lacked coverage and had done nothing about it, or simply didn't know their coverage.

Ethical Responsibility

Such a head-in-the-sand attitude, quite frankly, is a violation of a lawyer's professional ethics. Failure to reasonably anticipate and be prepared to service clients in the wake of a disaster is arguably a failure in the overall duty to act competently or in the best interests of your client.

There is a first-party side (affecting your firm directly) and a third-party side (affecting your clients) to this. A variety of first-party computer security disasters can lead to loss, such as a breach of security and unauthorized access to your systems, which damages your data or vandalizes your Web site, rendering you inoperable that day. This latter scenario may also lead to a third-party

loss to those clients whose reliance on your system is key to their livelihood — a perfect example would be clients who depend on being served through an extranet. All of these situations would impact your firm financially and are considered first-party losses.

When a third party is injured or harmed and your firm is responsible, a third-party lawsuit will likely be filed against you. This can include such exposures as identity theft or the invasion of your clients' privacy. Another area of exposure is Web site content and the infringement of a third party's intellectual property.

A hacker could access your system, grab your e-mail database and client mailing list and use your system to send out damaging malicious code, such as a computer virus or worm.

Alternatives

Many insurers do not provide specialized coverage for these unique exposures, or will try to take a Band-Aid approach by providing endorsements to traditional policies, such as property, fidelity and professional liability insurance.

The only really effective way to ensure that your firm and clients will not suffer loss through a computer disaster is cyberinsurance — a specialized form

of computer insurance coverage that insurance organizations such as American International Group, Chubb and Lloyd's of London have offered since the late 1990s.

An effective cyberinsurance policy can handle the first-party and third-party liabilities that your firm faces in a computer security disaster. These are typical kinds of coverage that are available:

First-party business interruption covers revenue lost during system downtime caused by accidents and security breaches. Losses during catastrophic regional power outages are typically excluded, but that's little different from standard exclusions for floods or other "acts of God."

First-party electronic data damage covers recovery costs associated with compromised data, such as virus infections.

First-party extortion covers ransom demands of hackers who claim to control systems or data and threaten to do serious harm.

Third-party network security liability covers losses associated with the compromise and misuse of data for such purposes as identity theft and credit card fraud.

Third-party (downstream) network liability covers judgments from lawsuits initiated by those harmed by denial-of-service attacks and viruses sent out over your system.

Third-party media liability covers infringement and liability costs associated with Internet publishing, including Web sites, e-mail and other interactive online communication.

Purchase Options

Cyberinsurance usually costs more than conventional liability or business interruption insurance. Unlike traditional insurance policies, cyberinsurance has no standard scoring system or actuarial tables for pricing premiums. Each insurance company has its own way of grading customers, with methods varying according to the type of insurance. Before insurers will provide a policy quote, they usually require potential cyberinsurance purchasers to fill out a questionnaire detailing the steps they've already taken to ensure computer security—firewalls, laptop computer encryption, antivirus protection and similar common-sense steps that all firms should take.

If you are interested in cyberinsurance, you should first review your current coverage. Are you spending too much on the traditional plans, such as property, and errors and omissions, when more of your firm's worth resides in unprotected data? If so, you need to understand not only what your data is worth to you, but how your systems affect your firm's bottom line. You should attempt to quantify how much you could lose from a computer disaster. Insurance costs money, so calculate the income loss so you can make better-informed decisions. Ultimately, the greatest loss may be in client confidence and resulting disciplinary action. ■

Attorney Edward Poll is the principal of Venice, Calif.-based LawBiz Management Co. and Edward Poll & Associates Inc. He is the author of the LawBiz Blog, www.lawbizblog.com.

THE CONNECTICUT
LAW TRIBUNE

Subscribe Today!
(860) 527-7900

Law Firms Open Virtual Offices For Offline Profit

Second Life's legal disputes are fertile ground for tech-savvy lawyers

By **JOHN BRINGARDNER**
ALM Media

In December, Judge Richard Posner of the 7th U.S. Circuit Court of Appeals attended a conference sponsored by Creative Commons, the nonprofit alternative copyright foundation, to promote his new book, "Not a Suicide Pact: The Constitution in a Time of National Emergency." Over the course of the question-and-answer session, Posner gave the assembled group his thoughts on topics ranging from the USA Patriot Act to copyright protection in a digital world.

The judge's words were punctuated by the occasional heckler throwing exploding fireballs from the sky. Posner was also distracted by a 6-foot raccoon. The giant animal claimed to be an intellectual property attorney from Washington, D.C. "I like your tail," Posner told him.

The event took place entirely within Second Life, a three-dimensional online virtual world created in 2003 by Linden Research, Inc., a small San Francisco startup doing business as Linden Lab. The 67-year-old judge's appearance in the world via a bespectacled avatar, or digital character, highlighted Second Life's growing significance as both social forum and marketing tool. The questions asked by Posner's audience for the most part were very serious. What place does the fair use doctrine have in Second Life? How should property rights be distinguished from IP rights in a virtual world?

More than 2.5 million people have visited Second Life, with 15,000-20,000 playing at any given time. Each person has an avatar that they use to walk, fly or teleport around islands full of clubs, shops and businesses that other users have created. Second Life is often grouped with online games known as MMORPGs, or massively multiplayer online role-playing games, such as Blizzard Entertainment's 7 million-player World of Warcraft. But Second Life differs from other MMORPGs in several crucial respects that have both helped to make it a success and opened it to a host of new legal disputes in an area still largely uncharted by the courts.

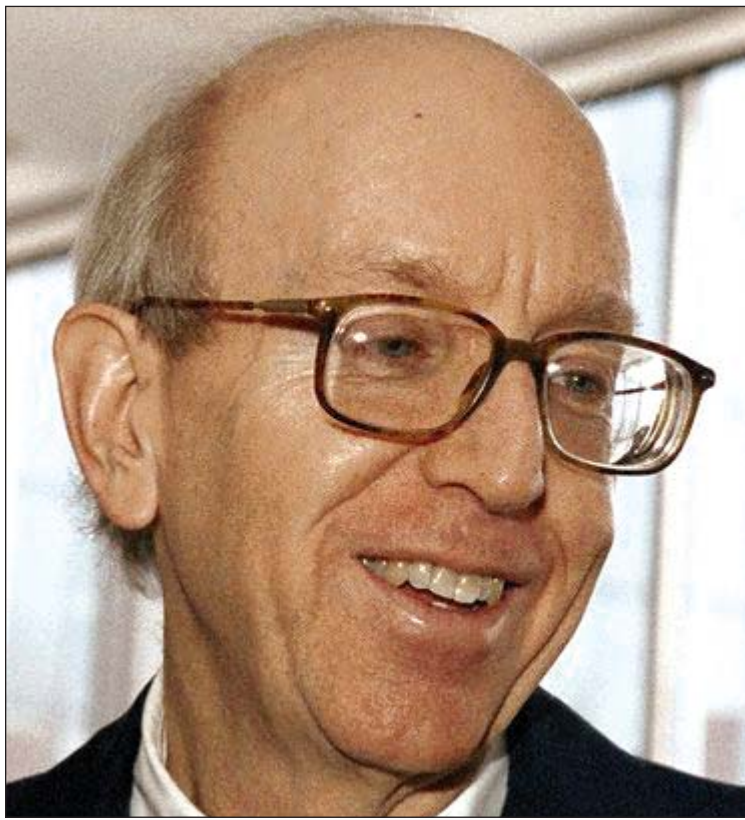
Real Money Invested

Instead of showy graphics and rapid-fire gameplay, Linden chief technology officer Cory Ondrejka decided that Second Life would offer its players something no other video game company had: intellectual property rights over their own creations within the virtual world. Players can endlessly customize their avatars and set up businesses on the virtual land they buy.

He was right, but it is the presence of real money invested in Second Life that has attracted so much attention. Second Life residents can buy and sell each other's creations using so-called Linden dollars. Where other games like Warcraft have long had unsanctioned gray markets where players buy and sell virtual goods for real cash, Linden made the market a fundamental

aspect of Second Life. It is an economy that currently trades more than \$1 million each day, at a floating exchange rate of about 270 Linden dollars to the U.S. dollar. Players can use a credit card or PayPal to buy and sell currency through the company's LindeX currency exchange. They can also use third-party online exchanges from companies like IGE Ltd., or even eBay Inc., to trade their virtual goods and currency.

Second Life's vibrant economy has encouraged corporate America to get virtual. MTV Networks opened a club in Second Life. Then American Apparel



Judge Richard Posner, of the 7th U.S. Circuit Court of Appeals, participated in a digital world speaking event, where he promoted his new offline book.

The American Lawyer File Photo

opened a T-shirt store, selling its digital, sweatshop-free clothing to avatars for about one U.S. dollar. Toyota Motor Corp. sells digital Scion cars, which it encourages residents to customize. IBM moved in last December and bought 12 new virtual islands, opening all but one to the public and reserving the last as a business meeting place for IBM employees.

These companies pay Linden a commission on transactions and rent on the virtual land they occupy, often hiring third parties to build out their virtual real estate. Their presence also prefigures a future for Second Life that goes beyond entertainment and small business. Its founders see this online world as the next phase of the Internet, the evolution from Web 2.0's social networking sites and wikis, or collaborative Web sites, to Web 3.0, where Web surfers who want to buy a book on Amazon.com would walk into a 3-D virtual bookstore instead of clicking through the Amazon site. Even if Second Life is eventually eclipsed by some future competitor, the legal precedents it helps establish will affect the future of online development.

Linden's Ondrejka and its CEO Philip Rosedale, both of whom declined to comment for this story, have publicly made much of the fact that their terms of service

agreement "recognizes residents' right to retain full intellectual property protection for the digital content they create in Second Life, including avatar characters, clothing, scripts, textures, objects and designs." Linden's IP policy says these rights are enforceable both within the game and offline, for both nonprofit and commercial ventures. As Linden's Web site states: "You create it, you own it—and it's yours to do with as you please."

Sounds simple, but what does that mean in practice? The Linden terms of service agreement has little precedent,

mous view of its users' IP, its end-user license agreement reserves the right to shut down any user's account at any time.

"There's no way, under the law, that you can get away with the forfeiture penalty clause that they think they have," says Archinaco.

Archinaco calls the company's actions a troubling precedent. "Assume [Bragg] is the worst human being on the entire planet," says Archinaco. "Does that mean they can go back and take the property he owns, sell it to the highest bidder and keep the money for themselves? No."

After the Bragg case was filed, Linden updated its terms of service agreement to explicitly state that the company retains ownership of player accounts and related data, "regardless of intellectual property rights you may have in content you create or otherwise own."

High Stakes, Novel Threats

The stakes are getting higher: Opening shop in Second Life is the corporate marketing trend du jour, and in December, Linden statistics showed 90 avatars earning more than \$5,000 each month. Also in December, a German woman, Aileen Graef, announced that she had earned \$1 million from Second Life real estate investments by her avatar, Anshe Chung, building on an initial investment of \$9.95 two years before. Anshe Chung Studios Ltd. now has 20 employees in Germany and China developing virtual real estate and creating fashion designs.

But residents such as Chung who create outfits, jewelry or pets for sale to other avatars faced a day of reckoning on November 13, when a new program called CopyBot was unleashed. An open source group called libsecondlife had been creating new software tools for Second Life with Linden's blessing, including one program that could make temporary clones of other avatars. When an unknown programmer altered the group's open source code to compile a program to make permanent clones, CopyBot was born. Within hours of its first reported use, designers and shop owners stopped selling en masse to avoid the risk of copied inventory. Second Life's economy ground to a halt.

Ondrejka decided that Linden would add time stamps to show when users had created their content as a way of distinguishing fakes from original creations, and he encouraged the use of Creative Commons attribution licenses, which allow free copying and modification of works, as long as they are attributed in the manner specified by the author or licensor.

Within days of the CopyBot outbreak, players were forced to click through a new agreement that specifically banned the use of such software. Protesting shopowners have reopened their businesses, and the most visible evidence of the CopyBot's disruption is the ubiquity of anticopying mea-

says New York's Kenyon & Kenyon associate S. Gregory Boyd, who coedited "Business & Legal Primer for Game Development." "It isn't like movie film law, which has been established for decades. We're looking for precedent and doing the best we can."

Enforceable Legal Rights

That uncertainty opened the door to Linden's first lawsuit. In May 2006, Marc Bragg, a solo attorney in West Chester, Pa., and one-time Second Life denizen, filed a complaint against Linden in the court of common pleas of Chester County, Pa. Bragg had discovered a loophole in the game's virtual land auction system and bought properties on the cheap before other players could make a bid. Linden eventually caught on and kicked him out. Bragg sued, arguing that the company was blocking him from \$8,000-worth of in-game assets, the "land" that he owned.

Bragg's lawyer, Jason Archinaco, is also an online game enthusiast. A partner in Pittsburgh firm White and Williams, Archinaco doesn't dispute that his client was in the wrong for his land purchases. But he says the case highlights a discrepancy in the Second Life terms of service. While Linden management espouses a magnani-

FRCivP RULE 37(F)

Destroyed E-Data Won't Lose Spoliation Sanctions

Safe-Harbor in New Rules May Be Tricky To Find

By **JONATHAN C. SCOTT**

While the new federal rules governing electronic discovery appear, on the surface, to offer parties a relatively simple means of avoiding discovery sanctions should discoverable electronic information be destroyed, the new rules, in reality, are not so simple.

Prior to the codification of guidelines regarding

Among the range of sanctions that are possible are those known as spoliation sanctions. In such a case the party that failed to preserve evidence relevant to the case will face a trial in which the jury will be instructed that it may infer that the un-produced evidence was damaging to that party's case and supported the claims of the adverse party.

Such an instruction is extremely damaging to the

the loss be in good faith to claim the safe harbor protection will make the availability of sanctions for the destruction of electronic evidence a fertile ground for litigation.

In pertinent part, FedRCivP 37(f) provides:

"Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

This language seems to suggest that a party not the subject of litigation could adopt a document-retention policy that provided for the routine and frequent destruction of electronic evidence and thereby generally be immune from civil sanctions when the party became a litigant in federal court and was unable to produce relevant electronic evidence because of that policy.

The rule should not be interpreted in such absolute terms. Inclusion of a requirement of good faith places the issue of the reasonableness of the party's conduct squarely before the court for its determination.

In that reasonableness assessment, the court will likely consider:

- whether the party adopted a policy of destroying core electronic information central to its business more frequently than documents less critical to business operations;
- whether at the time of the destruction the litigant reasonably anticipated that the documents might be needed for future reference;
- whether the destruction occurred after the party was put on notice of a potential claim in which the documents would be relevant in a subsequent proceeding or after a discovery demand or evidence preservation demand was made;
- the time and circumstances of the destruction;
- whether the party was at fault;
- whether the documents destroyed were required by law to be maintained because of industry record keeping requirements in order to confirm compliance with agency regulations.

In the leading 2nd Circuit authority on the subject, *Residential Funding Co. v. DeGeorge Financial Co.*, 306 F3d 99 (2d Cir. 2002), the court deemed an adverse inference instruction appropriate where the party failed, without good cause, to preserve and produce

■ See **RULE 37(F)** on PAGE 8



The applicability of the safe-harbor provision for routine operational loss is likely to be at issue in every case in which a litigant seeks to excuse its inability to produce relevant electronic documents because of its document retention policy.

electronic discovery in Federal Rules Rules 26 and 37 of the Federal Rules of Civil Procedure, effective Dec. 1, 2006, the federal courts addressed a litigant's obligations with respect to preservation and production of electronic evidence on a case-by-case basis.

Under existing precedent, where a party who created electronic documents either delays or fails to produce relevant materials to the opposing party, a district judge has substantial discretion in crafting a sanction which takes into consideration the nature of the violation.

Jonathan C. Scott is the senior partner of the law and technology services firm Scott & Scott, LLP. He is the chair of the litigation section of the firm. Aimee Hitchner and Lawrence R. Lassiter, litigators in the firm, assisted in the preparation of this article.

litigant's case and may be far worse than the inference that the jury would have drawn if the evidence was produced.

This article addresses the likely interplay between the new version of Rule 37 and the existing framework for sanctions.

Good Faith Requirement

While the newly promulgated FedRCivP 37(f) appears to provide a safe harbor protecting the party against sanctions for the routine destruction of electronic evidence, except in exceptional circumstances, the committee notes qualify that language. The qualification requires that for the safe harbor provision to apply, the loss of evidence must have been in good faith and that the exception cannot be used to exploit the new rule. The juxtaposition of an extraordinary circumstances standard against a requirement that

Make The
Write
Connections

Contact: Scott Brede, Editor In Chief
(860) 527-7900 x 642; email: sbrede@alm.com
Inquire about our editorial calendar for 2007

Contribute an article on
substantive law to
The Law Tribune

Next:
Construction Law



Hanging A Shingle In Online Virtual World

■ From **LAW FIRMS** on PAGE 5

tures that can slow activity in Second Life. As avatars move about the virtual world, they now frequently encounter scripts, or software code, placed near shops to disable the CopyBot before it can be used. The scripts appear as text shouted at residents, and now punctuate conversations between players—Second Life's equivalent of e-mail spam.

Second Life's potential copyright and trademark problems go beyond CopyBot. In Second Life, "copying of brand names and designs is rife," says Philip Cooper, a British IP attorney whose firm, Crossguard, maintains a virtual office there. "You can buy a virtual Ferrari or DKNY fashion garment."

Will the same brand owners that have spent millions trying to crack down on counterfeit goods in real-world venues like China be forced to take the fight to Second Life, too? Kenyon & Kenyon's Boyd says Second Life and other MMORPGs are enjoying a honeymoon period when it comes to IP infringement and other types of regulation. "In the next decade, these worlds will certainly garner more attention as their population grows and as the value of virtual property within the worlds increases," he says. "That increased attention will almost certainly result in companies searching those

games more diligently for infringement."

Avatar Attorneys

With all these legal controversies, it's no wonder that some lawyers are setting up shop in Second Life. Cooper's avatar, Philip Gloucester, wears a suit and tie, and appears to be a close digital representation of the man himself, albeit with more digital hair. Cooper was one of the first IP attorneys to open a virtual office in Second Life, where he solicits online and offline clients for his U.K.-based firm, Crossguard. He typically spends his working hours in the real world, playing in Second Life at night. Crossguard's spacious virtual office has Old Master reproductions hanging on the walls, and recently had a Christmas tree and a Santa Claus out front. Potential clients press a button in the office to page Cooper via e-mail.

(Not every self-described law office in Second Life is what it purports to be, however. Avatar attorney Onoto Arbusto advertises a practice called Second Life Legal Services. But in teleporting to Arbusto's office this December, a visitor discovered instead a gingerbread "Kinky Cottage" and found his own avatar forced into a suggestive pose on all fours. As throughout the Internet, adult content is sometimes difficult to avoid in Second Life.)

Cooper's more conservative office attracted the attention of other IP lawyers entering the virtual realm. Stevan

Lieberman, a partner in D.C. IP boutique Greenberg & Lieberman, has had an office in Second Life since March 2006. He met Cooper online, and the two now send offline referrals to each other. They're also generating business within Second Life. Lieberman has written standard business contracts for two clients in Second Life, programmers he met through their avatars. He spoke with one of his clients by phone; the other matter he handled exclusively via Second Life and e-mail. He created a special payment structure for that client, accepting 90 percent of his bill in U.S. dollars, and the rest in Linden dollars. Lieberman used the virtual cash to furnish his Second Life office, a wooden octagon floating 300 feet in the air.

Second Life Arbitration

What has taken more of Lieberman's time, however, is trying to create a Second Life arbitration system, to better handle internal disputes. One complicating factor is jurisdiction. Linden currently operates under California and U.S. law. British IP attorney Cooper says that virtual worlds like Second Life need a form of international arbitration. "If I get ... an Australian operating a business in Second Life, asking me, a U.K. attorney, how he can best protect his business within Second Life, how do I answer him?" he says, citing one query that he has received. But Cooper sees a model in the uniform dispute resolution policy

(UDRP) for Internet domain names. Created in 1999 by the Internet Corporation for Assigned Names and Numbers (ICANN) in cooperation with the World Intellectual Property Organization, the UDRP created an international solution to issues like cybersquatting of domain names that were difficult or impossible to resolve in regional courts.

Cooper, Lieberman and other interested avatars, including the Second Life Bar Association and many non-lawyers, are now working together to formalize online arbitration as a required first step to handle Second Life disputes, without resort to real courts and their costs. Together they are lobbying Linden to include arbitration in its terms of service agreement. Meanwhile, Lieberman's group is introducing its proposed arbitration into the virtual world, hoping that other users will try it out and find it fair and useful.

Kenyon & Kenyon's Boyd applauds the effort: "It's too complicated to resolve these [disputes] outside of [Second Life]. Hopefully you're going to see arbitrations."

Until the company creates its own dispute resolution system, Lieberman says that disgruntled users can threaten real-world court battles against fellow residents and Linden itself to protect their assets. "Second Life is no different than the rest of the universe," says Lieberman. "People will go where they have the greatest advantage." ■

THE TEXT.

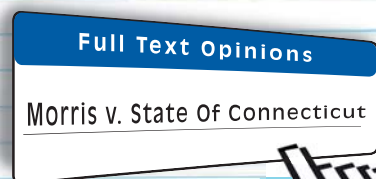
THE FULL TEXT.

AND NOTHING BUT THE FULL TEXT.

SO HELP YOURSELF.

Subscribe today: www.ctlawtribune.com

For additional info: (860) 527-7900



1. Subscribe to www.ctlawtribune.com
— just sign up, no credit card needed

2. Search decision digests
(by title, subject, judge, etc.)

3. Find one... download the FULL TEXT
INSTANTLY with ONE CLICK

THE CONNECTICUT
LAW TRIBUNE
Online ALM

ProNetworkSupport.com



Microsoft
GOLD CERTIFIED
Partner

- Network Installation
- Network Management
- Network Consulting
- Network Support

Voted #1 in Network Support.

Our Proactive Support makes your computers and networks secure, efficient, and always available.

ProNetworkSupport.com

a division of **VISUAL TECHNOLOGIES, INC.**

117 Oak Street, Hartford, CT 06106
860.251.8003 x133

Rule 37(f)'s 'Discovery Obligation': An Untested Concept

■ From **DESTROYED** on PAGE 6

complete electronic evidence for use by the opposing party, even though the party did not intentionally destroy the evidence.

An electronic document retention or destruction policy that is unreasonable because it fails to preserve information that might be reasonably anticipated to be needed in future or pending litigation likely would also fail the requirement under FedRCivP 37(f) that the operational loss of electronic documents be the result of good faith and be reasonable.

It would be unwise for a company or municipal entity to interpret this rule as a broad-based immunity against sanctions for the routine destruction of electronic evidence.

Scope Of E-Data Discovery

It is commonly understood that destroying relevant evidence after entry of a federal court order requiring its production to the adverse party will support severe sanctions. There is nothing in Rule 37(f) creating a safe harbor in those circumstances, because the continuation of a policy that causes the destruction of evidence subject to an outstanding court order is unreasonable as a matter of law.

The committee notes to the Rule 37(f) make reference to the destruction of evidence related to "a discovery obligation" without defining the contours of that obligation. In particular, it is unclear as to whether Rule 37 spoliation sanctions will only be available if the destruction of relevant electronic evidence occurs after the action is filed or whether, consistent with prior precedent, the courts will hold that a party's obligation to preserve evidence encompasses a pre-suit responsibility to maintain evidence for another's use in a reasonably foreseeable litigation.

Even in the absence of a court order, litigants have an obligation to preserve relevant evidence for the use of the adverse party.

If electronic documents are destroyed as a result of a document-retention policy when federal litigation is reasonably anticipated as a result of a document-retention policy, the court may find that the policy was unreasonable and the safe harbor provision of Rule 37(f) inapplicable.

A parties' document-retention obligations also derive from record-keeping regulations intended to verify compliance with business, entity or industry-specific regulations. Examples include regulations by the Securities and Exchange Commission, regulations requiring a broker-dealer to maintain records of electronic communications for a certain time period and state document retention rules related to documents created by municipal entities. While it is true that a private litigant in a federal civil action seeking such information because it is relevant to his or her case against a party has no private right of action under industry record keeping rules, there is a strong argument that a document retention policy that destroys evidence for use in federal court

that the party was required by law to independently maintain is unreasonable as a matter of law.

The new federal rules concerning electronic discovery provide a helpful framework as well as a process for dealing with how electronic documents will be handled in federal litigation.

A Delicate Balance

The new rules attempt to strike a balance between many competing considerations. But like any other rules providing guidance for the courts and litigants, the

rules must be considered in the broader context of the interests advanced or impaired, as well as the policies involved. An aggressive document-destruction policy may be perceived by a court as unreasonable if it impairs the fact-finding function without a countervailing policy which justifies it. A document-retention policy that requires a business or entity to retain every electronic communication may be perceived by the court as being unduly burdensome.

The applicability of the safe-harbor provision for routine operational loss is

likely to be at issue in every case in which a litigant seeks to excuse its inability to produce relevant electronic documents because of its document retention policy. Companies and entities that have taken the time pre-suit to measure the reasonableness of their document-retention policies against industry standards, to ensure compliance with applicable document retention compliance regulations and to review and modify those policies to be more inclusive when federal court litigation is anticipated or filed, are those most likely to win the safe-harbor fight. ■

New Rules of Civil Procedure?

We've been turning electronic discovery challenges into opportunities since 1999

What do you do when faced with the volume and complexity of electronic information? We have the solution to your electronic discovery problems!

Introducing **eddiesm**, the next generation of document management.

eddiesm converts your electronic information into a fully searchable database. You provide us with the data, and we do the rest!



225 Asylum Street Hartford, CT 06103 (860) 256-0220 www.ipsllc.net