

News Highlights in This Issue:

Social Networking Site Immune Under CDA	19
NAGTRI/NCJRL Offer Wireless Training	14
Michigan to Require Forensics License	24
Study: 80% of Business PCs Unsecured	26
Use of GPS Device Without Warrant OK	19
Cyber-Criminals Quicker to Exploit Flaws	27
Ct. Privacy Expectation in Text Messages	20
New Hampshire Update Sex Offender Law	24
Few Companies Use Hosted Data Archiving	26
Delayed Search of Cell Phone Held Valid	21
California Enacts Cyber Harassment Law	25
Project for New Internet Gets Funding	27
New York to Require Video Game Rating	26
Sending Hyperlink Not Distributing Porn	22
Vermont Bans Online Tobacco Sales	25
Poll: E-Discovery Becoming Unmanageable	29
Blanket as "Instrument" Enough for Charge	23
Missouri Cyber Harassment Law Signed	25
Cybersecurity Big Part of 2009 Budget	29
New DC Law Prohibits Spam	25

Table of Contents

<u>Features</u>	2
The New Frontier: Virtual Worlds	
New: Wireless for Attorneys Course	
<u>AGs Fighting Cyber Crimes</u>	14
AG Goddard Prosecuting Offender	
California AG Sue Online Pyramid	
AG Blumenthal: Video Game Responds	
Florida AG's Unit Arrests Pornographer	
AG Bennett Says Predator Sentenced	
Illinois AG Settles With E-Tailer	
AG Carter Sues Online Seller	
Kansas AG Unveils Net Safety Site	
AG Conway's Team Arrests Predator	
Massachusetts AG: Possession Arrest	
AG Cox's Team Arrests Predator	
Mississippi AG: Possession Plea	
AG Nixon Sues Online Replica Company	
Montana AG's E-safety Site Awarded	
AG Ayotte Sues Online Shoe Store	
New Jersey AG: Predator Sentenced	
AG King's Agents Confiscate Illegal CDs	
New York AG Gets ISP Agreement	
AG Cooper Gets E-tailer Judgment	
Oklahoma AG Gets E-Bay Fraudster	
AG McMaster Says Predator Arrested	
Texas AG Charges Net Ticket Broker	
AG McDonnell Unveils Net Safety Video	
Wisconsin AG Wins Pornographer Appeal	
<u>In the Courts</u>	19
MySpace Not Liable Under CDA	
No Privacy in Military Computer	
Warrantless Use of GPS Device OK	
Privacy in Text Messages Found	
Search Pursuant to Warrant Valid	
Delayed Search of Cell Phone Lawful	
Porn Via Hyperlink Not Distribution	
Vulgar Blog Punishment Appropriate	
"Blanket" Sufficient for Charge	
Adding Spoliation Claim Approved	
Subpoena Won't Avoid ED Deadline	
Issues Not Ripe for Litigation Hold	
<u>Legislation Update</u>	24
Michigan Requires Forensics Licenses	
New Hampshire Updates Offender Law	
New California, Missouri E-bullying Laws	
Vermont Bans Online Tobacco Sales	
DC Enacts Anti-Spam Law	
Senate Committee Ok's ICAC Bill	
New York Requires Video Game Rating	
California Senate Ok's Texting Bill	
Mandatory 911 Service Bill Enacted	
<u>News You Can Use</u>	26
80% of Business PCs Unsecured	
New Internet Projects Gets Funds	
Laptop Bags May Stop Airport Hassle	
Anti-Spam Group Issues ISP Guidance	
Report Says Botnet Spam Unstoppable	
Cybercrime Akin to Organized Crime?	
Cybersecurity Large Part of '09 Budget	
House Committee Probes Net Tracking	
CEOs: E-Date is UNmanageable	

The Cyber Crime Newsletter is developed under the Cyber Crime Training Partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi School of Law. It is written and edited by Hedda Litwin, Cyber Crime Counsel (hlitwin@naag.org, 202-326-6022).

This project was supported by Grant No. 2000-DD-VX-0032 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the authors and do not represent the official position of the United States Department of Justice.

The views and opinions of authors expressed in this newsletter do not necessarily state or reflect those of the National Association of Attorneys General (NAAG). This newsletter does not provide any legal advice and is not a substitute for the procurement of such services from a legal professional. NAAG does not endorse or recommend any commercial products, processes, or services. Any use and/or copies of the publication in whole or part must include the customary bibliographic citation. NAAG retains copyright and all other intellectual property rights in the material presented in the publications.

In the interest of making this newsletter as useful a tool as possible for you, we ask that you keep us informed of your efforts. Additionally, we would like to feature articles written by you. Please contact us with information, proposed articles and comments about this newsletter. Thank you.

**The New Frontier in the Fight
Against Online Economic Scams
and Internet Threats to
Children: Virtual Worlds and
Second Life**

John S. Grant IV

Most Internet users are familiar with the social networking sites Facebook and MySpace. These sites are a favorite Internet destination for many teens and young adults, many of whom post much of their lives on these sites for a wide audience to view. However, another type of Internet forum has been gaining ground on the popularity of these social networking sites. These fora are known as “virtual worlds,” one of the most popular of which is Second Life.

But what is a virtual world? It has been defined as “an interactive simulated environment accessed by multiple users” through the Internet.¹ There are at least thirty virtual worlds in

existence,² and there are multiple types of virtual worlds, with one of the most popular becoming the “online community building” type, which includes Second Life (SL).³ Another type of virtual world is the gaming type, which includes the widely popular World of Warcraft.⁴ This virtual world is akin in many ways to traditional, pre-virtual world video and computer games but with much broader capability for interaction with other players.

However, it is fair to say that SL is much less of a game, and more closely resembles “real life.” Second Life users, unlike users of online games, have no set of objectives to complete.⁵ Rather, SL users primarily join SL to communicate and interact with other users and/or to market products.⁶ However, there are many problems that can occur in such an

² See *id.*

³ See *id.*

⁴ Mark Wallace, *A Virtual Holiday in the Virtual Sun*, N.Y. TIMES, Oct. 28, 2005, <http://www.nytimes.com/2005/10/28/travel/esca pes/28virtual.html>.

⁵ Bobby Glushko, *Tales of the Virtual City: Governing Property Disputes in Virtual Worlds*, 22 BERKELEY TECH. L. J. 507, 524 (2007).

⁶ *Id.*

¹ Virtual Worlds Review, What is a Virtual World?, <http://www.virtualworldsreview.com/info/whatis.shtml>.

environment, including various types of online scams and children being exposed to harmful content or child predators. For this reason, SL and other similar virtual worlds present many new and unique challenges for policy makers, prosecutors, and law enforcement officials.

This article will begin by providing an introduction to virtual worlds and SL. Discussion will then turn to two specific topics—SL monetary transactions and SL content that might be harmful to children (including sex, drugs and violence). It concludes, in the last two sections, with thoughts on various legal and cyber crime issues pertaining to virtual worlds, with a focus primarily on SL.

Introduction

First of all, what about virtual worlds and Second Life distinguishes them from online social networks such as Facebook and MySpace? There is a fundamental difference in the way that the two types of social phenomena operate and the options provided to users. Social networking sites allow users to post pictures of themselves online, create mini biographies of themselves, chronicle their daily lives, and instant message other users in real time. Although social networks allow for a great deal of social interaction, most of it is not done in real time. Also, aside from links to video clips, everything on social networking sites is two-dimensional.

In contrast, virtual worlds like Second Life—rather than allowing their users to tell about their actual lives—offer users the ability to “live” virtual lives in a three-dimensional online environment resembling the real world. Second Life users, who are known as

“residents,”⁷ establish an online identity through a virtual character known as an “avatar,” which residents can use to explore SL’s world and to interact in real time with other SL residents.

To become a part of SL’s world, residents must first register, download SL software and create an avatar. Residents are required to choose a unique name not chosen by any other SL user, which becomes their identity within SL. Creating a single basic account on SL is free,⁸ although SL residents can, and many do, spend money in order to have additional options within SL (more on this in the next section).

Residents can navigate through SL by maneuvering their avatars through the vast expanse of SL’s world, which encompasses many thousands of virtual acres that are lined with three-dimensional content largely paralleling the natural and man-made scenery found in the real world—trees, mountains, oceans, buildings, cities, etc.⁹ Residents can navigate through SL by having their avatars physically fly through the air or by teleporting directly to their desired locations.¹⁰

Residents are afforded many options for how they can spend time on SL. First, residents can interact socially

⁷ Second Life Wiki, Origin of the Term ‘Resident,’ [http://wiki.secondlife.com/wiki/\(search for “resident”\)](http://wiki.secondlife.com/wiki/(search%20for%20%22resident%22)) (last accessed July 27, 2008).

⁸ Official Second Life Site, Frequently Asked Questions, <http://secondlife.com/whatis/faq.php>.

⁹ Matt Gross, *It’s My (Virtual) World and Welcome to It!*, N.Y. TIMES, Nov. 3, 2006, [http://www.nytimes.com/\(search for “it’s my virtual world”\)](http://www.nytimes.com/(search%20for%20%22it’s%20my%20virtual%20world%22)).

¹⁰ Samantha Gross, *Take a Virtual Vacation: Travel in Second Life*, USA TODAY, May 11, 2007, http://www.usatoday.com/tech/gaming/2007-05-11-virtual-vacation_N.htm.

by using their avatars as intermediaries to communicate and interact with other avatars logged in at that particular time.¹¹ Second, residents may choose to have their avatars employed and may choose from almost any conceivable occupation—anything from tattooist to dancer, landscaper, gunsmith, or architect.¹² Many avatars own businesses and employ other avatars.¹³ Third, residents can have their avatars engage in almost any conceivable “real life” daily activity—anything from fixing their hair to organizing their closet.¹⁴ These activities are done primarily for enjoyment, and residents who consider these sorts of activities mundane really have no reason to do them. Fourth, residents can have their avatars participate in recreational activities such as shopping for virtual items, fishing for virtual fish, or visiting virtual nightclubs.¹⁵ Avatars can even get married in virtual wedding ceremonies.¹⁶

Virtual Economics

Second Life is owned by Linden Lab, a San Francisco-based company. The company was created in 1999 to

create a three-dimensional online world where users would interact with each other and build the virtual landscape.¹⁷ Linden Lab released Second Life in 2003.¹⁸

Second Life has grown quickly since its release. By 2005, Linden Lab announced that Second Life had grown to over 100,000 users; the figures had reached one million by October 2006 and eight million by July 2007.¹⁹ According to Second Life’s website, the number of SL user accounts as of July 2008 exceeded 14 million.²⁰ However, these figures may be deceptively high as an indicator of the total number of users, as users are allowed to create more than one account.²¹ The total number of avatars that log in during a given week may be as many as 450,000,²² and the number of avatars logged in at any given time regularly exceeds 60,000.²³ Linden Lab currently more than 200 employees in the United States, Europe and Asia.²⁴

How does Linden Lab make money from Second Life? Second Life users may opt either to reside in SL for

¹¹ Marco R. della Cava, *Utopia Goes Digital*, USA TODAY, Aug. 21, 2005, http://www.usatoday.com/life/lifestyle/2005-08-21-virtual-utopia_x.htm.

¹² Official Second Life Site, Business Opportunities, <http://secondlife.com/whatis/businesses.php>.

¹³ Alexandra Alter, *Is This Man Cheating on His Wife?*, THE WALL STREET JOURNAL, Aug. 10, 2007, <http://online.wsj.com/public/article/SB118670164592393622.html>.

¹⁴ Shira Boss, *Even in a Virtual World, ‘Stuff’ Matters*, N.Y. TIMES, Sep. 9, 2007, <http://www.nytimes.com/> (search for “virtual world stuff matters”).

¹⁵ Wallace, *supra* note 4.

¹⁶ *Id.*

¹⁷ Linden Lab Home Page, <http://lindenlab.com/> (hereinafter “Linden”).

¹⁸ Second Life Grid, What is Linden Lab?, http://secondlifegrid.net/resources/fact_sheet/lindenoverview.

¹⁹ *Id.*

²⁰ Official Second Life Site, Economic Statistics, http://secondlife.com/whatis/economy_stats.php (last accessed July 27, 2008) (hereinafter “Economic Statistics”).

²¹ See Official Second Life Site, Terms of Service, § 2.4, <http://secondlife.com/corporate/tos.php> (hereinafter “Terms of Service”).

²² Economic Statistics, *supra* note 20.

²³ Posting of Mitch Wagner to Information Week’s Digital Life Weblog, http://www.informationweek.com/blog/main/archives/2008/04/linden_lab_name.html (Apr 22, 2008, 7:35 p.m.).

²⁴ Linden, *supra* note 17.

free on a “basic account,” or sign up for a “premium account,” which requires paying money to Linden Lab for an upgraded package. A premium account can be obtained for as little as \$6 per month if the user is willing to pay for one year’s worth of SL’s services.²⁵ Although the majority of Second Life users have basic accounts,²⁶ a substantial amount of money is spent within Second Life daily.

Second Life has its own system of currency known as Linden dollars, which can be used to purchase virtual items within SL. If residents buy a premium account, they obtain a one-time grant of 1000 Linden dollars, and they will receive a 300 Linden dollar per week allowance.²⁷ If residents opt to enter Second Life for free on a basic account, they receive a one-time 250 Linden dollar lump sum.²⁸ In order to own virtual land, however, residents must purchase a premium account.²⁹

There are many resources outside of SL that provide the service of converting U.S. dollars to Linden dollars and vice versa, which can also be done through Linden Lab’s currency exchange service, called LindeX.³⁰ Although the exchange rate between these two currencies fluctuates based upon economic principles, the exchange rate is

typically about 250 Linden dollars to one U.S. dollar.³¹

Omitted from the list in the last section of what residents can do with their avatars is acquiring virtual property. Virtual property can include anything from virtual pairs of shoes, to virtual skin for avatars, to virtual real estate. Although it may seem odd to some that people are willing to spend money on items that are composed of computer pixels, virtual property is increasingly becoming a booming industry.

Many transactions for virtual property occur daily within Second Life. Residents can enter transactions directly with other residents in order to exchange U.S. currency for Linden dollars or virtual property. Such transactions typically involve one avatar finding another and proposing a transaction, the two avatars negotiating, and the deal being finalized through an instant message screen and an Internet payment system such as PayPal.³² Additionally, transactions for virtual property can happen on the Internet outside of SL,³³ which has resulted in businesses forming to sell SL items.³⁴ These items, once purchased, can then of course be brought into SL.

It has been estimated that more than \$1.5 billion worth of user-to-user

²⁵ Official Second Life Site, Membership Plans, <http://secondlife.com/whatis/plans.php> (last accessed July 22, 2008) (hereinafter “Membership Plans”).

²⁶ Second Life Premium Growth Flat Over Past 12 Months, <http://secondlife.reuters.com/stories/2008/07/02/second-life-premium-growth-flat-over-past-12-months/> (July 2, 2008, 1:21 a.m. PDT).

²⁷ Membership Plans, *supra* note 25.

²⁸ *Id.*

²⁹ *Id.*

³⁰ Official Second Life Site, Currency Exchange, <http://secondlife.com/whatis/currency.php>.

³¹ *Id.*

³² Online Business Journal of the University of Pennsylvania’s Wharton School, *The New New Economy: Earning Real Money in the Virtual World* (Nov. 2, 2005), <http://knowledge.wharton.upenn.edu/> (search “virtual worlds”).

³³ *Id.*

³⁴ See Posting of Mitch Wagner to Information Week’s Digital Life Weblog, <http://www.informationweek.com/news/software/hosted/showArticle.jhtml?articleID=199701944> (May 26, 2007, 12:01 a.m.) (describing Second Life sex industry) (hereinafter “Wagner’s Blog Post”).

transactions take place per year within virtual worlds at large.³⁵ During the month of June 2008, about \$29 million in user-to-user transactions occurred just within SL.³⁶ Linden Lab does not earn a commission from transactions that occur between SL residents.³⁷

With real money to be made, many people have quit their real jobs in order to become virtual entrepreneurs on SL.³⁸ At least one person has become a millionaire in such an endeavor.³⁹ With this practice of earning a “virtual income” becoming more commonplace, the U.S. Congress has become involved in investigating how these incomes should be taxed.⁴⁰

In addition, real-world businesses have ventured onto SL. Mainly, these companies establish a presence there in order to float new product ideas and to advertise products rather than to generate revenue.⁴¹ These businesses

pay Linden Lab a small leasing fee for virtual land from which to run their headquarters within SL but pay tech companies large amounts to develop their virtual land—\$100,000 to \$5 million, according to one report.⁴² Among the corporate giants that have entered SL is Toyota, which has sold Scion cars to SL residents for about 300 Linden dollars, or a little more than one U.S. dollar.⁴³ Other companies with SL accounts include Coca Cola, Nike, Dell and IBM.⁴⁴ Furthermore, nonprofit and religious organizations, political campaigns, and even educational institutions (which teach classes through SL) have established a presence on SL.⁴⁵

Many have predicted that the upward trend in the creation of avatars will dramatically continue to rise in the coming years. For example, one Internet research firm has predicted that eighty percent of frequent Web users and Fortune 500 companies will inhabit a virtual world such as SL by 2011.⁴⁶

³⁵ Albert C. Lin, *Virtual Consumption: A Second Life for Earth?*, 2008 B.Y.U.L. Rev. 47, n.221.

³⁶ Second Life Sees Record Usage But Bleeds Paid Accounts, <http://secondlife.reuters.com/stories/2008/07/08/second-life-sees-record-usage-but-bleeds-paid-accounts/> (Jul 8, 2008, 2:10 p.m. PDT).

³⁷ Bob Tedeschi, *Awaiting Real Sales From Virtual Shoppers*, N.Y. TIMES, June 11, 2007, <http://www.nytimes.com/> (search for “virtual shoppers”).

³⁸ Kathleen Craig, *Making a Living in Second Life*, WIRED, Feb. 8, 2006, <http://www.wired.com/gaming/virtualworlds/news/2006/02/70153>.

³⁹ Posting by Roger Parloff to CNN’s Legal Pad Weblog, <http://money.cnn.com/blogs/legalpad/2006/11/anshe-chung-first-virtual-millionaire.html> (Nov. 27, 2006, 11:25 a.m.).

⁴⁰ US Congress Launches Probe into Virtual Economies, <http://secondlife.reuters.com/stories/2006/10/15/us-congress-launches-probe-into-virtual-economies/> (Oct. 15, 2006, 10:43 p.m. PDT).

⁴¹ See Reena Jana & Aili McConnon, *Second Life Lessons: Real-world Businesses*

Face the Costs and Learn the Benefits of Setting up Shop in the Online Universe, BUSINESS WEEK, Oct. 30, 2006, http://www.businessweek.com/playbook/06/1030_1.htm.

⁴² See Tedeschi, *supra* note 37.

⁴³ Peter Valdes-Dapena, *Real Cars Drive into Second Life*, CNN, Nov. 18, 2006, http://www.cnn.com/2006/AUTOS/11/17/2nd_life_cars/index.html.

⁴⁴ Consultaglobal, Corporations Now Present At Second Life, <http://consultaglobal.wordpress.com/2007/04/22/corporations-now-present-at-second-life/>.

⁴⁵ Albert C. Lin, *Virtual Consumption: A Second Life for Earth?*, 2008 B.Y.U.L. Rev. 47, 85-86.

⁴⁶ *Id.*

Sex, Drugs and Violence

Before getting into the specifics of content harmful to children that is on Second Life, there should first be an explanation of how the content on SL is created. Practically everything on SL is created by its residents, with Linden Lab only furnishing the landscape on which to build.⁴⁷ Residents can create almost anything imaginable in building the appearance of their avatars or creating changes to the virtual landscape.⁴⁸

Linden Lab provides the building tools to allow users to create content.⁴⁹ These tools can be used to manipulate the primary building blocks of SL content, graphic primitives, or “prims,” by altering their shape, color or texture.⁵⁰ All content creation can be done within SL,⁵¹ although separate programs such as Adobe Photoshop can also be used in the process.⁵² Second Life provides an added incentive for users to create content by allowing users to retain copyrights to their creations.⁵³

Not only are the possibilities for creation nearly endless, but there is very little “red tape” to step through, as no pre-approval or submission process exists.⁵⁴ Therefore, if someone can imagine something and is tech savvy enough to create it, the virtual item, whatever it may be, most likely can become part of SL.

As one might expect, with people from around the globe having this

largely unencumbered freedom of possibility, there is a substantial amount of violence, drugs and sexually explicit content that is created. First, a great deal of cybersex takes place on SL, which essentially involves avatars providing their operators with a visual image of virtual humans engaging in various sexually explicit acts.⁵⁵ The sexually explicit content that has been reported to be within SL includes virtual lap dances, orgies, sex clubs and sex slaves.⁵⁶ Residents can create avatars that are of the opposite sex, and they can experiment with homosexuality.⁵⁷ There are also escort services on SL that engage in virtual prostitution.⁵⁸ Finally, residents can purchase virtual genitalia for their avatars from shops in SL.⁵⁹

Second, the content on SL includes drugs and violence. A recent post on YouTube provides evidence of the various drug paraphernalia and drugs that are present on SL, including marijuana, cocaine, acid, mushrooms and heroine.⁶⁰ Another YouTube video shows an avatar committing suicide within SL by jumping off of a building.⁶¹ YouTube searches also indicate that

⁵⁵ Yvonne K. Fulbright, *FOXSexpert: Cybersex--Taking on a Whole New 'Life,'* FOXNEWS, Mar. 3, 2008, <http://www.foxnews.com/story/0,2933,334681,0.html>.

⁵⁶ *Id.*

⁵⁷ Wagner's Blog Post, *supra* note 34.

⁵⁸ *Having Sex*, WIRED, October 2006, <http://www.wired.com/wired/archive/14.10/slentertainment.html>.

⁵⁹ *Id.*

⁶⁰ Youtube.com, Drugs Dope Weed Acid Shrooms Heroin Cocaine Bongs & More, <http://youtube.com/watch?v=LWq8aG7UC8s> (warning: this video contains visual depictions of many user created virtual drugs).

⁶¹ Youtube.com, Death of and [sic] Avatar-Second Life, <http://youtube.com/watch?v=UJLyTB3KRSw> (warning: this video shows an avatar committing suicide).

⁴⁷ Wallace, *supra* note 4.

⁴⁸ Todd David Marcus, *Note: Fostering Creativity in Virtual Worlds: Easing the Restrictiveness of Copyright for User-Created Content*, 52 N.Y.L. Sch. L. Rev. 67, 73 (2007).

⁴⁹ *Id.* at 87.

⁵⁰ *Id.* at 73.

⁵¹ *Id.* at 87.

⁵² *Id.* at 73.

⁵³ *Id.* at 68.

⁵⁴ *Id.* at 87.

various weapons, including assault weapons, are present on SL.⁶²

Second Life does contain some safeguards to protect minors from this potentially harmful content. There is a separate area of the Second Life's virtual world for teens,⁶³ and Second Life maintains "community standards" that participants in Teen Second Life agree to follow. These standards include that teen residents should not harass each other and that all teen activity on its site should be "PG," which means free from offensive language, nudity, and "strong violence."⁶⁴ Teen Second Life has an in-world mechanism for reporting abuses, and Second Life claims that reports of abuse will be individually investigated.⁶⁵ Although generally violators of the community standards are given a warning, repeat violators may be suspended or expelled from Second Life.⁶⁶ Additionally, teens are prohibited by Second Life's Terms of Service from entering into the adult area.⁶⁷

In order to join the adult SL, users must certify that they are at least eighteen years old.⁶⁸ Users who are over eighteen are prohibited by SL's Terms of Service from accessing the teen area, and adults found in the teen area may face expulsion from SL.⁶⁹ However, SL's Terms of Service agreement

⁶² Youtube.com (search for "second life weapons") (warning: some of these results contain graphic violence).

⁶³ Official Teen Second Life Site, What is Teen Second Life?, <http://teen.secondlife.com/whatis>.

⁶⁴ See Official Teen Second Life Site, Community Standards, <http://teen.secondlife.com/footer/cs>.

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ Terms of Service, *supra* note 21, at § 2.2.

⁶⁸ *Id.*

⁶⁹ *Id.*

explicitly states that SL makes no guarantees that residents remain in their respective age appropriate areas: "Linden Lab cannot absolutely control whether minors gain access to the Service other than the Teen Area . . . [or] whether adults gain access to the Teen Area."

Second Life has come under fire of late for the harm that it could cause to children who can potentially manage to access the adult areas of the site. According to Representative Mark Kirk (R-Illinois), who has called for a ban of SL from public schools and libraries, the content on SL that children could be exposed to includes substantial violence, including the ability of avatars to purchase assault weapons and commit suicide.⁷⁰ In addition, Kirk has stated that the sexual content available includes rape, and residents can choose for their avatar "to rape or be raped."⁷¹ While acknowledging that some SL features require the user to provide credit card information, Kirk has stated that much of the sexually explicit content can be accessed for free and is "readily available."⁷² In addition, he has expressed concern that there is no age verification software in place to prevent children from accessing the adult areas of the site.⁷³

The CEO of Linden Lab, Philip Rosedale, who has recently announced that he is stepping down from his

⁷⁰ Posting by Walter Alarkon to Briefing Room Weblog, <http://briefingroom.thehill.com/tag/second-life/> (May 15, 2008, 12:02 p.m.).

⁷¹ *Id.*

⁷² Posting to Virtual World News Weblog, <http://www.virtualworldsnews.com/2008/05/representative.html> (May 7, 2008, 09:37 a.m.).

⁷³ *Id.*

position,⁷⁴ recently testified before a congressional committee, and received questions regarding minors' ability to access harmful content.⁷⁵ When asked how Linden Lab prevents adults from accessing Teen Second Life, Rosedale testified that Linden encourages teens to warn Linden of any SL avatar whose behavior indicates that he or she is not a teen.⁷⁶ He testified that Linden takes some precautions to verify age, including providing features that ask for credit card and telephone information and features that require users to verify that they are the appropriate age before being permitted to use SL software.⁷⁷ However, he stated that Linden does not receive social security numbers or driver's license numbers.⁷⁸

Second Life also has been criticized for permitting adults to create child avatars on its site. As mentioned earlier, SL users can create almost any conceivable sort of character, and assuming the identity of a child is one available option. While some have defended child avatars as being merely an avenue for "role playing," SL users have reported that cybersex involving virtual pre-pubescent children was once common on its site.⁷⁹ However, Linden Lab has stated that "sexual ageplay," which is sexual content appearing to

involve children, violates its Community Standards,⁸⁰ and has stepped in and begun shutting down "sexual ageplay" areas of its site.⁸¹ Nevertheless, SL seems to continue to allow adults to pose as children on its site.⁸²

Consumer Protection and Intellectual Property Legal Issues

Although virtual property is a developing area with little established caselaw, it is an area that is likely to see much litigation in the near future. Second Life residents have sued each other and Linden Lab for many disputes that have arisen in-world through SL, ranging from copyright infringement actions over resident ideas and creations to disputes between residents over the ownership of virtual property.⁸³ Without attempting to compile an exhaustive list of virtual property lawsuits that have been brought, the following are a couple of examples.

In 2006, Marc Bragg filed what was reportedly the first virtual property lawsuit against Linden Lab.⁸⁴ Bragg alleged that directly after he acquired a parcel of land, the land was confiscated, and he was terminated from SL, which in effect confiscated all of his virtual

⁷⁴ Posting by Adam Reuters to Second Life News Center Weblog, <http://secondlife.reuters.com/stories/2008/03/14/exclusive-rosedale-to-step-down-as-linden-lab-ceo/> (Mar. 14, 2008, 9:29a.m. PDT).

⁷⁵ Online Virtual Worlds: Applications and Avatars in a User-Generated Medium (webcast of congressional hearing from April 1, 2008), http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.040108.VirtualWorlds.shtml (hereinafter "Virtual Worlds Hearing").

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ Wagner's Blog Post, *supra* note 34.

⁸⁰ Posting of Ken D. Linden to Second Life Weblog, <http://blog.secondlife.com/2007/11/13/clarification-of-policy-disallowing-ageplay/> (Nov. 13, 2007, 5:10 p.m.).

⁸¹ Wagner's Blog Post, *supra* note 34.

⁸² Second Life Wiki, http://wiki.secondlife.com/wiki/User:Marianne_McCann/Child_Avatars (last accessed July 27, 2008).

⁸³ Alter, *supra* note 13.

⁸⁴ Aili McConnon, *Virtual World, Real Courtroom*, BUSINESS WEEK, October 16, 2006, http://www.businessweek.com/magazine/content/06_42/c4005010.htm.

assets.⁸⁵ The complaint included allegations of fraud, conversion and violation of various consumer protection laws.⁸⁶ Linden Lab claimed that Bragg had acquired his virtual land through an exploit in the system.⁸⁷ According to one source, Bragg had prematurely initiated virtual land auctions within SL, allowing him to purchase the land for a substantially lower price.⁸⁸ In a published opinion, the District Court for the Eastern District of Pennsylvania denied Linden Lab's motion to compel arbitration,⁸⁹ but the parties eventually settled the lawsuit.⁹⁰

In another lawsuit, Eros, LLC, which sells various sex products within SL, filed a copyright infringement lawsuit for copying and selling its products to SL residents without authorization.⁹¹ It took four months of investigation—which included hiring a private detective,⁹² and issuing subpoenas to Linden Lab, PayPal and other companies to trace SL activity to the proper computer⁹³—to identify

Robert Leatherwood, a nineteen year old, as the SL resident who controlled the SL avatar named Volkov Catteneo.⁹⁴ Eros then amended its complaint to name Leatherwood as a defendant in the case.⁹⁵

As mentioned earlier, users may retain intellectual property rights in their creations. As a result, Eros was able to sue Leatherwood for copying, and selling at a discounted price, one of its products—a virtual bed that allows SL avatars to have sex.⁹⁶ Leatherwood did not respond to the complaint and a default judgment was entered.⁹⁷ However, Leatherwood eventually conceded that he was in fact the owner of the avatar named Volkov Catteneo, and the parties reached a settlement, which provides that Leatherwood is to refrain from further copying.⁹⁸

Unauthorized copying within SL has been made possible through various programs including the infamous CopyBot, which, in 2006, was released within SL by a third party.⁹⁹ The

⁸⁵ Bragg v. Linden Research, Inc., 487 F.Supp.2d 593, 597 (E.D. Pa. 2007).

⁸⁶ *Id.* at 597 n.8.

⁸⁷ *See id.* at 597.

⁸⁸ Glushko, *supra* note 5, at 525.

⁸⁹ Bragg v. Linden Research, Inc., 487 F.Supp.2d 593, 612-13 (E.D. Pa. 2007).

⁹⁰ Linden Lab Settles Bragg Lawsuit, <http://secondlife.reuters.com/stories/2007/10/04/linden-lab-settles-bragg-lawsuit/> (Oct 4, 2007, 4:06 p.m. PDT).

⁹¹ Citizens Media Law Project, <http://www.citmedialaw.org/threats/eros-llc-v-doe> (July 27, 2008) (link to complaint available by clicking on PDF document at bottom of webpage).

⁹² Volkov Catteneo: Yes, I am Robert Leatherwood, <http://secondlife.reuters.com/stories/2008/03/06/volkov-catteneo-yes-i-am-robert-leatherwood/> (Mar 6, 2008, 12:37 p.m. PDT) (hereinafter "Volkov Catteneo").

⁹³ Posting by Benjamin Duranske to Virtually Blind Weblog,

<http://virtuallyblind.com/2007/11/29/eros-leatherwood-default/> (Nov. 29, 2007).

⁹⁴ Volkov Catteneo, *supra* note 92.

⁹⁵ Posting by Benjamin Duranske to Virtually Blind Weblog, <http://virtuallyblind.com/2007/10/25/robert-leatherwood-identified-eros/> (Oct. 25, 2007).

⁹⁶ Jonathan Richards, *Second Life Sex Bed Spawns Virtual Copyright Action*, TIMES ONLINE, July 4, 2007,

http://technology.timesonline.co.uk/tol/news/tech_and_web/article2025713.ece.

⁹⁷ Citizens Media Law Project, <http://www.citmedialaw.org/threats/eros-llc-v-doe> (July 27, 2008) (link to Order for Judgment by Consent available by clicking on PDF document at bottom of webpage).

⁹⁸ Posting by Benjamin Duranske to Virtually Blind Weblog, <http://virtuallyblind.com/2008/03/14/leatherwood-settlement/> (Mar. 14, 2008).

⁹⁹ Kurt Hunt, Note: *This Land Is Not Your Land: Second Life, CopyBot, and the*

program has allowed SL users to copy any in-world item at no cost.¹⁰⁰

For its part, Linden Lab has announced that its Terms of Service ban the use of the CopyBot and other similar programs, and using such a program may result in user expulsion from SL.¹⁰¹ Also, Linden Lab has recently responded to users' complaints that others have pirated their content by removing the content under the authority of the Digital Millennium Copyright Act.¹⁰²

Second Life has also seen at least one instance of an alleged large scale fraud. An in-world bank, known as Ginko Financial, promised in-world investors a return on their investments amounting to more than 40 percent annually.¹⁰³ The bank was criticized as an illegal "Ponzi scheme," which is an "investment vehicle that pays off old investors with money from new ones."¹⁰⁴ The bank eventually went bankrupt, owing investors over 700,000 U.S. dollars.¹⁰⁵ Although there were rumors floating of an impending lawsuit,¹⁰⁶ no

Looming Question of Virtual Property Rights, 9 Tex. Rev. Ent. & Sports L. 141, 143-44 (2007).

¹⁰⁰ *Id.*

¹⁰¹ *Id.* at 148.

¹⁰² Pirated Content Deleted from Second Life, <http://secondlife.reuters.com/stories/2008/06/17/pirated-content-deleted-from-second-life/> (June 17, 2008 2:01p.m. PDT).

¹⁰³ The Illinois Business Law Journal, *Virtual Bank, Real Scam?*, (Feb. 12, 2007) http://iblsjournal.typepad.com/illinois_business_1aw_soc/2007/02/virtual_bank_re.html.

¹⁰⁴ Unable to Pay Depositors, Ginko Ceases Banking Operations, <http://secondlife.reuters.com/stories/2007/08/09/unable-to-pay-depositors-ginko-ceases-banking-operations/> (Aug 9, 2007, 7:27 a.m. PDT).

¹⁰⁵ Posting by Benjamin Duranske on Virtually Blind Weblog, <http://virtuallyblind.com/2008/01/21/ginko-financial-selling-server-on-ebay/> (Jan. 21, 2008).

¹⁰⁶ *Id.*

such lawsuit appears to have materialized.

Linden Lab's CEO has claimed that Linden Lab attempts to prevent fraud by examining all transactions involving more than 10 U.S. dollars.¹⁰⁷ Since the Ginko Financial collapse, SL has banned in-world banks without "government registration statement or financial institution charter."¹⁰⁸

Currently, virtual property rights are defined by the end user license agreements (EULAs) to which virtual world members are required to agree in order to join most virtual worlds.¹⁰⁹ These EULAs are primarily enforced at the discretion of the company owning the virtual world.¹¹⁰

Second Life is no different, as its EULA gives Linden Lab broad discretion to regulate virtual property. Its Terms of Service contains the following: "you understand and agree that Linden Lab has the right . . . to remove any content (including your content) in whole or in part at any time for any reason or no reason, with or without notice and with no liability of any kind."¹¹¹ This broad discretion to SL's developer seems to be in tension with a section of SL's Terms of Service that allows users to retain property rights in their creations,¹¹² and Linden Lab has been criticized for profiting from the sale

¹⁰⁷ Eric Reuters, <http://secondlife.reuters.com/stories/2008/04/01/osedale-discloses-fbi-griefing-probe-to-congress/> (Apr 1, 2008, 2:05 p.m. PDT).

¹⁰⁸ Posting of Ken D. Linden to Second Life Weblog, <http://blog.secondlife.com/2008/01/08/new-policy-regarding-in-world-banks/> (Jan. 8, 2008, 10:43 a.m.).

¹⁰⁹ Glushko, *supra* note 5, at 514.

¹¹⁰ *Id.* at 517.

¹¹¹ Terms of Service, *supra* note 21, at § 5.3 (capital letters changed to lowercase).

¹¹² *See id.* at § 3.2.

of virtual property without adequately protecting the interests of virtual property owners.¹¹³

The bottom line, though, is that further litigation will be necessary in order to determine to what extent virtual property rights will be protected, and to what extent Linden Lab can regulate virtual property under its EULA and Terms of Service notwithstanding SL users' claims to such property.¹¹⁴ How a court would resolve almost any virtual property dispute is speculative at this point. As Benjamin Duranske, a lawyer who is the primary contributor to the blog *Virtually Blind*, has observed, even the simplest of questions, such as "whether currency in virtual worlds should be equated with real world currency" and "whether virtual land can be meaningfully equated with real property" are still without any real or helpful answers.¹¹⁵

Child Predators and Child Pornography Issues

There is relatively little to no mention as to actual prosecutions for sexually-related crimes against children committed by way of virtual worlds or Second Life. Researching this article uncovered only scattered attempts to prosecute such crimes and, for the most part, only in foreign jurisdictions. For example, one investigation was undertaken by German authorities in an attempt to apprehend those responsible for sexually explicit content depicting

virtual children within SL.¹¹⁶ Possession of virtual pornography is illegal under German law.¹¹⁷ Linden Lab has assisted German law enforcement in their investigation.¹¹⁸

Although the possibility in the U.S. for the prosecutions related to virtual child pornography has been questionable at best because of the First Amendment, a recent U.S. Supreme Court decision is worth discussing briefly on this point. The case of *United States v. Williams*, a 7-2 decision that was handed down this term, has implicated that prosecution for the "pandering or solicitation" of virtual child pornography may be possible.¹¹⁹

At issue in the case was a provision of the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 ("the Act").¹²⁰ The provision prohibits, inter alia, knowingly pandering or soliciting material that "reflects the belief, or that is intended to cause another to believe" that the material contains an "obscene visual depiction" of a minor engaged in "sexually explicit conduct."¹²¹ The Court held that this statute was not substantially overbroad.¹²²

Congress passed the Act in response to the invalidation of the Child Pornography Protection Act of 1996 in the case of *Ashcroft v. Free Speech*

¹¹⁶ *Second Life 'Child Abuse' Claim*, BBC, May 9, 2007, <http://news.bbc.co.uk/2/hi/technology/6638331.stm>.

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ *Cf. United States v. Williams*, 128 S. Ct. 1830, 1836-37, 1842 (2008).

¹²⁰ *Id.* at 1836.

¹²¹ *Id.* at 1836-37 (citing 18 U.S.C. §2252A(a)(3)(B)).

¹²² *Id.* at 1841.

¹¹³ Hunt, *supra* note 99, at 149.

¹¹⁴ See Posting by Benjamin Duranske to Virtually Blind Weblog, <http://virtuallyblind.com/2007/08/23/vb-commentary-active-suits-unsettled-issues/> (Aug. 23, 2007).

¹¹⁵ *Id.*

Coalition.¹²³ The statute at issue in that case, the *Williams* majority explained, had been invalidated in part because it extended beyond prohibiting “pandering,” and prohibited the possession of virtual child pornography.¹²⁴

The *Williams* case created a notable distinction. It appears that offering to provide or requesting to obtain (i.e., pandering or soliciting) virtual child pornography receives no First Amendment protection, at least under certain circumstances.¹²⁵ On the other hand, possessing virtual child pornography that was pandered by someone else appears to still be protected.¹²⁶ Even though transfers of virtual child pornography may be proscribed, however, prosecutions for such transfers within SL will still be difficult under the First Amendment because “[a] crime is committed only when the speaker believes or intends the listener to believe that the subject of the proposed transaction depicts real children . . . [and virtual] child pornography will be as available as ever, so long as it is offered and sought as such, and not as real child pornography.”¹²⁷

As to the issue of child predators, researching this article revealed no specific case involving the prosecution of a child predator for activity related to Second Life. However, the U.S. Congress has shown some concern on this issue. On April 1, 2008, the U.S. House Energy and Commerce Committee’s Subcommittee on Telecommunications and the Internet

held the very first congressional hearing on virtual worlds, but its focus was primarily on SL.¹²⁸

At the hearing, members asked the CEO of Linden Lab, Philip Rosedale, about the process for locating child predators within SL. Rosedale responded that Linden has the ability to review the history of “communication, transactions, and behavior generally” of SL users.¹²⁹ However, according to Rosedale, Linden retains these records only for a period of several weeks.¹³⁰

Rosedale emphasized that the site is “aggressively self-policed” and that Linden actively investigates suspect in-world activity.¹³¹ He stated that there has been little SL activity of concern thus far, but he asserted that Linden has been proactive about notifying the authorities of the supposedly infrequent cases of suspect activity.¹³² He also testified that Linden has actively involved the FBI in investigating cyber crimes that have occurred within SL.¹³³

Conclusion

Although virtual worlds and Second Life provide many positive contributions to society today by allowing people to communicate and interact with each other in ways never before possible, these internet fora have spawned many problems as well. Second Life, in particular, has completely changed the concept of property ownership in a matter of a few

¹²³ *Id.* at 1842 (citing *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002)).

¹²⁴ *Id.* at 1836.

¹²⁵ *See id.* at 1842-43.

¹²⁶ *See id.* at 1836.

¹²⁷ *Id.* at 1844.

¹²⁸ Posting by Benjamin Duranske to Virtually Blind Weblog, <http://virtuallyblind.com/2008/04/01/congress-virtual-worlds/> (Apr. 1, 2008).

¹²⁹ Virtual Worlds Hearing, *supra* note 75.

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² *Id.*

¹³³ *Id.*

years, and it has created many risks to consumers never before encountered. In addition, SL poses an enormous threat to children—both in the potential for children to access adult content and in the potential for children to fall victim to online predators. What is troubling is that Linden Lab, however well intentioned, has determined what policies govern SL, and has “self policed” almost all aspects of SL with little outside intervention. Increased involvement by policy makers, prosecutors and law enforcement is needed in order to combat the very real injustices that are clearly occurring within this virtual world.

**THE COURSE YOU’VE BEEN
WAITING FOR IS HERE...
AND IT’S FREE**

The National Attorneys General Training and Research Institute (NAGTRI) joins with the National Center for Justice and the Rule of Law

(NCJRL) to announce the availability of “**Computer Crimes in the Wireless Age,**” an advanced course for prosecutors and civil enforcement attorneys alike to be held on October 21-23 at the University of Mississippi School of Law in Oxford, Mississippi. The course will focus on how to handle cases in which wireless devices are an integral part of the crime and the evidence. Topics to be covered include how the different technologies work, wiretaps, cell phone tracking, securing wireless devices and much more. There is no fee for assistant attorneys general, and most transportation costs will be reimbursed under the NAGTRI-NCJRL partnership.

A nomination form to attend the course is attached to the back of this e-newsletter. The course is expected to fill up quickly, so the earlier your nomination is received, the better will be your chance of acceptance.

AGs FIGHTING CYBER CRIMES

ED NOTE: Recently the Center for Democracy and Technology and the Center for American Progress issued a report which concluded that online fraud cases are given less priority by state Attorneys General than cases involving Internet crimes against children. Much of the report’s research and arguments are based on Attorneys General initiatives published over the years in our e-newsletters. While buried in one sentence of the report is a statement that the cases brought by Attorneys General that are reported in this e-newsletter are not “comprehensive,” it appears that the report’s findings are based on this small sample of cases. Our readers know that space and

readability concerns mandate that this e-newsletter limit its reporting of cases or initiatives brought by Attorneys General to one per state per issue. We are thus surprised that the report did not include the other publicly available cases brought by Attorneys General, which might have changed the report’s outcome.

ARIZONA

Attorney General Terry Goddard announced the indictment of David Green on charges of sexual exploitation of a minor and attempted sexual exploitation of a minor.

According to the indictment, investigators found 10 images and a movie containing pornographic images of children on Green's home computer. The indictment resulted from an investigation by Immigration and Customs Enforcement. If convicted on all charges, Green faces up to 240 years in prison. Assistant Attorney General Todd Lawson is prosecuting the case.

CALIFORNIA

Attorney General Jerry Brown, Jr. filed suit against YourTravelBiz.com, its affiliates and founders for operating an online pyramid scheme that recruited members with deceptive claims about earning large sums of money through online travel agencies. Members who join are compensated for each new person they enlist, but they actually earn nothing selling travel. Company records showed that there were more than 200,000 members who typically each paid more than \$1,000 per year: \$449.95 to set up an "online travel agency" and a monthly fee of \$49.95. Only 38 percent of members made travel commissions in 2007, and the median income was \$39 – less than one month's fee. Under California's unfair business practices statute, the company is liable for \$2,500 per violation. Attorney General Brown is also asking the court to bar the company from making false or misleading statements and to assess a civil penalty of at least \$15 million and at least \$10 million in restitution.

CONNECTICUT

Attorney General Richard Blumenthal announced that, in response to his concerns, JV Games, a video game production company, will remove all alcoholic references in its "Beer Pong" game, including the name. Attorney General Blumenthal also sent a letter to the Entertainment Software Rating Board, urging them to change the rating for the game from suitable for children 13 years of age and older to adult only.

FLORIDA

Attorney General Bill McCollum's CyberCrime Unit, together with the Lake County Sheriff's Office, arrested Barry Landstedt, a facilities coordinator for Lake County, on two charges of child pornography possession. The pornography was discovered during a routine undercover investigation. A search warrant was then executed at Landstedt's home, and investigators seized his computer. Landstedt admitted to downloading and viewing child pornography images. His computer will undergo additional forensic analysis, and additional charges could be made depending on the outcome. If convicted, Landstedt faces up to five years in prison on each count. Both the Unit and the Sheriff's Office are members of the Central Florida Internet Crimes Against Children Task Force.

HAWAII

Attorney General Mark Bennett announced that Ronald Young, a self-employed carpenter, was sentenced to 10 years in prison for Electronic Enticement of a Child in the First Degree, as required by Hawaii's new law, and must also register as a sex offender. Young used the Internet to solicit a law enforcement officer who he believed to be a 13-year-old girl and was arrested when he arrived at the arranged meeting place. He pled guilty to the crime. The investigation of Young involved law enforcement agents from the Hawaii Internet Crimes Against Children Task Force, including Attorney General Bennett's Department and the Honolulu Police Department.

ILLINOIS

Attorney General Lisa Madigan entered a \$405,000 settlement with StoresOnline, Inc. and Galaxy Mall, inc., two Utah-based companies that offered assistance in establishing online businesses but failed to fully provide the promised assistance. The settlement will provide refunds to the consumers who had signed on with the companies. Attorney General Madigan's suit alleged that the companies promised to provide the start up

assistance during an eight-hour training session that included sales pitches and testimonials and advertised that no computer or prior business experience was necessary. Consumers each paid more than \$2,600 for services, but the companies failed to provide the technical support and services promised. The agreement also requires the companies to make specific fee and service disclosures. It requires them to include their name and address and the name of the entity providing the training session in all solicitations.

INDIANA

Attorney General Steve Carter sued Trina and Wendy Hasty, Virginia Hoffman and Dana Laster for failing to deliver tanning products sold to at least 12 people online. The defendant used more than one dozen business names to sell their products, including Lotion Town, Tanning Products, Indoor Tanning Lotion, Best Indoor Tanning, Cheaper Lotions and Payless Lotions. The suit seeks reimbursement for consumers who did not receive products, civil penalties of up to \$5,500 per violation and investigative costs.

KANSAS

Attorney General Steve Six unveiled www.NetSafeKansas.com, a new Internet safety web site aimed at educating children, teens, parents and others about online dangers. The site has separate sections for each audience, with the site for kids and teens focusing on cyberbullying, social networking and cyberstalking. The site for parents contains information on how to better protect their kids online, while the consumer section addresses issues such as Internet scams.

KENTUCKY

Attorney General Jack Conway's investigators arrested Billy Williams in connection with a cybersafety predator sting they conducted in the southern part of the state. Williams, who had been communicating online with a decoy, was taken into custody by Attorney General Conway's Department of Criminal Investigations agents and

officers of the Williamsburg Police Department when he arrived to meet with whom he thought was a 12-year-old girl. He was charged with unlawful transaction with a minor in the first degree, a Class C felony, punishable by five to 10 years in prison.

MASSACHUSETTS

Attorney General Martha Coakley announced that Kenneth Conti of Johnston, Rhode Island was arrested and arraigned on one count of Possession of Child Pornography. Attorney General Coakley's office launched an investigation after Conti's former employer contacted them, and investigators found that Conti had images of child pornography on USB drives and in binders at his work cubicle. He was arrested at his parents' house in Johnston by the Johnston Police Department and brought back to Massachusetts by state troopers assigned to Attorney General Coakley's office. The case is being prosecuted by Assistant Attorney General Christopher Kelly of Attorney General Coakley's Cybercrime Division.

MICHIGAN

Attorney General Mike Cox's investigators arrested Daniel Everett for using the Internet to arrange a meeting for sex with a minor. Everett chatted online with whom he thought was a 14-year-old girl he met in a chatroom but who was actually an agent, and was arrested at the pre-arranged meeting place. He is charged with one count of Child Sexually Abusive Activity and one count of Using the Internet to Commit Child Sexually Abusive Behavior, both 20-year felonies.

MISSISSIPPI

Attorney General Jim Hood announced that John Boyles pled guilty to two counts of fondling children under the age of 16 years and one count of possession on his computer of sexually explicit images of an actual child under age 18. Boyles was sentenced to serve five years on the child pornography plea and two years each on the fondling pleas, which will run concurrently. Upon

release, he will serve 15 years on probation, with five of those years under supervision. He was also ordered to pay \$2,000 to the Crime Victim's Compensation Fund, a fine of \$10,000 and a fine of \$1,000 to Attorney General Hood's office, plus court costs.

MISSOURI

Attorney General Jay Nixon sued John Adams, who does business as Missouri Cannon Works, for violating the state's Consumer Protection Act by advertising Civil War replicas on his web site, requiring customers to make advance payments with personal checks or wire transfers and failing to provide the merchandise or make refunds. The lawsuit asks for restitution for consumers, preliminary and permanent injunctions to prohibit Adams from further violations and to pay appropriate penalties and costs to the state.

MONTANA

Attorney General Mike McGrath's "Safe in YourSpace" cybersafety web site received a WAGGY award for Best Consumer Outreach at the annual Conference of Western Attorneys General (CWAG). The web site, which features a teen snowboarder "surfing" the Internet, includes information for young people, parents and educators. It contains a glossary of terms, links to national resources and information on cyberbullying, Internet predators, instant messaging and social networking sites. It was created in cooperation with the Montana Safe Schools Center at the University of Montana.

NEW HAMPSHIRE

Attorney General Kelly Ayotte announced that a preliminary injunction was issued against an Internet business, My Shoe Store, Inc., d/b/a My Shoe Store.com or Lord John's Footwear, and its sole director and president, Michael Kyriannis of New York. My Shoe Store was a registered New Hampshire corporation until its recent dissolution. Attorney General Ayotte's lawsuit claimed that Kyriannis immediately charged consumers' credit

or debit cards for shoes ordered online despite the items not being in stock. The business then failed to fill orders and provide refunds in a timely manner or not at all. Some customers received refunds by checks which bounced. Approximately 400 customers were affected. The preliminary injunction orders Kyriannis and his company to immediately cease and desist from accepting payment prior to shipping the ordered merchandise. The suit also requests restitution for affected consumers and fines for non-compliance with the previous Assurance of Discontinuance.

NEW JERSEY

Attorney General Anne Milgram joined Criminal Justice Director Deborah Gramiccioni in announcing that Christopher Frazee was sentenced to 364 days in jail as a condition of probation for manipulating an underage New Hampshire girl into posing nude on the Internet using a web camera. The sentence was pursuant to Frazee's guilty plea to endangering the welfare of a child. As part of the investigation, the New Jersey State Police Digital Technology Investigations Unit executed a search warrant and seized Frazee's computer, recovering nude images of the girl and logs of communications between Frazee and the girl. Deputy Attorney General Kenneth Sharpe of the Division of Criminal Justice Computer Analysis and Technology Unit represented the Division at the sentencing.

NEW MEXICO

Attorney General Gary King's Investigations Division Special Agents and forensic personnel executed a search warrant at Krazy Kat Music in connection with an investigation into illegally reproduced compact discs. They confiscated suspected illegally reproduced CDs, computers and other evidence at the scene. Investigators from the Recording Industry Association of America were also present during the raid. Selling more than seven "pirate" CD copies is a fourth degree felony under New Mexico law.

NEW YORK

Attorney General Andrew Cuomo announced that Cablevision, the largest Internet service provider on Long Island, agreed to immediately begin blocking customers' access to online child pornography. The company will also eliminate access to child pornography Newsgroups, a major supplier of illegal child pornography. Attorney General Cuomo met with Long Island parents to discuss his efforts. The announcement follows similar agreements with Comcast, AT&T, Verizon, AOL, Sprint and Time Warner Cable.

NORTH CAROLINA

Attorney General Roy Cooper announced that a consent judgment was submitted to the court under which Internet sales companies, iMergent, Inc. and StoresOnline, Inc. of Utah, agreed to change the representation of its products, including making clear that individuals who offer testimonials have been paid to do so and informing consumers of their right to cancel services. The companies claimed to help consumers set up an easy to use online business requiring little or no computer experience, which was incorrect as moderate technical skills are necessary. Their services cost \$2,700 for three web sites, plus a monthly hosting fee of \$24.95 per site. Both companies will pay refunds to consumers, and Attorney General Cooper's office has already obtained more than \$265,000 in refunds for state consumers. They will also be required to notify consumers in writing about their three-day right to cancel, which is extended to 15 days for consumers over the age of 65.

OKLAHOMA

Attorney General Drew Edmondson announced that Douglas Barry is facing four counts of violating the state Consumer Protection Act after an investigation by Attorney General Edmondson's Consumer Protection Unit. Barry operated You Bring It, We Sell It, a consignment store that sold merchandise on the Internet for consumers for a commission. He allegedly sold merchandise,

including a 1937 Dodge pickup, electronic equipment and a Suzuki motorcycle, on eBay for four consumers and then failed to remit the money from the sales. In all, Barry owed the consumers \$17,600.

PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit agents arrested Andrew Beck, who is accused of using Internet chat rooms to sexually proposition whom he believed were 13- and 14-year-old girls, but who were actually Unit undercover agents using the online profiles of children. Beck, who used the screen name "lovindad59," is charged with four counts of unlawful contact with a minor and one count of criminal use of a computer, all third degree felonies each punishable by up to seven years in prison and \$15,000 in fines. He will be prosecuted by Deputy Attorney General Michael Sprow of the Unit.

SOUTH CAROLINA

Attorney General Henry McMaster announced the arrest of Jordan Hicks in an undercover Internet sting conducted by the Oconee Sheriff's Office, a member of Attorney General McMaster's Internet Crimes Against Children Task Force. Arrest warrants allege that Hicks solicited sex on the Internet from whom he believed to be a 13-year-old girl, but who was actually an undercover Sheriff's deputy. Hicks was arrested when he arrived at the location where he had arranged to meet the "girl." The Anderson County Sheriff's Office, also a Task Force member, assisted with the arrest and the execution of a search warrant which resulted in the seizure of two computers. Hicks was arrested on one count of Criminal Solicitation of a Minor, a felony punishable by up to 10 years imprisonment, and one count of Attempted Criminal Sexual Conduct with a Minor, a felony punishable by up to 20 years imprisonment. The case will be prosecuted by Attorney General McMaster's office.

TEXAS

Attorney General Greg Abbott charged TicketCity Inc., an online ticket broker, with unlawfully deceiving 2008 Beijing Summer Olympics ticket purchasers. The company initially sold opening ceremony tickets for \$1,250 and promised to double the refund if it failed to deliver the pre-purchased tickets. Relying on the guarantee, consumers bought airline tickets, but TicketCity did not possess the tickets when they sold them and later informed consumers that their purchases and the 200 percent refunds would not be honored. Nevertheless, TicketCity continued offering opening ceremony tickets, this time starting at \$7,000 each. Attorney General Abbott seeks civil penalties of up to \$20,000 per violation of the Texas Deceptive Practices Act and actual damages to consumers who were financially harmed.

VIRGINIA

Attorney General Bob McDonnell joined Comcast and the Internet Keep Safe Coalition (iKeepSafe) to unveil a video that teaches children

and parents about online safety. The video explores the risks associated with the Internet and teaches parents and guardians how to become involved and take action to protect their children. It was debuted during an event at a Boys & Girls Club. Comcast and iKeepSafe also presented Attorney General McDonnell with an award for his work in keeping the state's children safe.

WISCONSIN

Attorney General J.B. Van Hollen announced that a court of appeals upheld the conviction of Gordon Sussman on two counts of Repeated Sexual Assault of a Child and 16 counts of Possession of Child Pornography. The court rejected Sussman's arguments that his trial counsel was ineffective and that the circuit court's admission of hearsay testimony was grounds for a new trial. Assistant Attorney General Daniel O'Brien handled the appeal.

IN THE COURTS

SOCIAL NETWORKING SITES AND LIABILITY CLAIMS

Doe v. MySpace Inc., 2008 WL 2068064 (5th Cir. May 10, 2008). The 5th Circuit Court of Appeal affirmed a decision of the U.S. District Court for the Western District of Texas, which found that a social networking site was entitled to immunity under the Communications Decency Act (CDA) § 230© for allegedly failing to institute adequate safety measures to prevent sexual assaults of minors and age verification policies. The Does argued that CDA § 230©(1) was inapplicable because their negligence claims did not implicate MySpace as a "publisher" protected by

the Act. The 5th Circuit rejected this argument, finding that despite the Does assertions that they only sought to hold MySpace liable for its failure to implement protective measures, their claims "speak to MySpace's role as a publisher of online third party-generated content, and thus CDA immunity would apply.

FOURTH AMENDMENT: SEARCH OF MILITARY COMPUTER

Us v. Larson, 66 M.J. 211 (C.A.A.F. April 25, 2008). John Larson, an Air Force Major, used his military office computer to download child pornography and chat with an

undercover officer posing as a 14-year-old girl. He arranged to meet the “girl” for sex and was arrested. Officers searched his computer and found the child pornography and records of the sexually explicit chats. At trial, Larson argued that the warrantless search of his military computer violated the Fourth Amendment and that the evidence obtained should be suppressed. A military judge rejected his claim, finding that 1) several personnel had keys to the office where the computer was located; 2) while Larson could secure the computer with a password, a system administrator could still access it; and 3) when Larson logged on, he was required to click on a statement that he understood the computer was government property, was for government use and that he agreed to monitoring. The judge found that Larson had no reasonable expectation of privacy in the computer and denied his motion to suppress. Larson sought review of the ruling, but the U.S. Court of Appeals for the Armed Forces affirmed.

FOURTH AMENDMENT:
WARRANTLESS USE OF GPS
DEVICE

People v. Weaver, 2008 WL 2277587 (N.Y.A.D. 3 Dept. June 5, 2008). The New York Supreme Court, Appellate Division, Third Department, found that a warrant is not required before police can affix a GPS device to a suspect’s vehicle. A police officer, in the course of investigating a series of burglaries, attached a GPS device without a warrant under the bumper of Scott Weaver’s van while it was parked on a public street. Based upon the data retrieved from the GPS, Weaver was arrested, charged with burglary and grand larceny and convicted. Weaver then appealed to the

appellate court, claiming that the trial court erred in denying his motion to suppress the evidence obtained from the warrantless placement of the GPS in his van. The Third Department relied on the principle that “where there is no legitimate expectation of privacy, there is no search or seizure” under the Fourth Amendment. It concluded that since constant visual surveillance of Weaver’s vehicle in plain view by police would have revealed the same information and been just as intrusive, and no warrant would have been necessary to do so, the use of the GPS did not infringe on any reasonable expectation of privacy and did not violate Weaver’s Fourth Amendment protections.

FOURTH AMENDMENT:
REASONABLE EXPECTATION OF
PRIVACY

Quon v. Arch Wireless Operating Co., Inc., 2008 WL 2440559 (9th Cir. June 18, 2008). The Ninth Circuit held that the City of Ontario, California violated the Fourth Amendment when police department officials viewed text messages sent by an employee. The court also ruled that the city’s service provider, Arch Wireless, violated the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-11, when it disclosed messages to individuals who were neither the addressees nor the recipients. Sergeant Jeff Quon consistently overran the 25,000 character monthly allotment on his departmental pager, but always paid the overage charges. However, despite the informal policy that messages would not be audited if the employee paid the overage charges, Quon’s police chief obtained transcripts of Quon’s text messages from a support specialist at Arch Wireless. The chief and three other department employees

reviewed the messages, many of which were personal and some of which were sexually explicit. Quon sued both the department and Arch Wireless in the U.S. District Court for the Central District of California, alleging both violations of the SCA and the Fourth Amendment. The district court held that Arch Wireless did not violate the SCA because it was a “remote computing service” under § 2702(a) and therefore committed no harm when it released the transcripts to its subscriber, the city. As to the Fourth Amendment claim, the district court held a jury trial on the sole issue of the police chief’s intent. The jury found was to determine the efficacy of the character limit, and the city was absolved of wrongdoing. On appeal, the Ninth Circuit reversed, finding that, based on prior experience paying for overages, Quon had a reasonable expectation of privacy in his text messages. As to the jury finding of the chief’s intent, the court found there were less intrusive ways of verifying the efficacy of the character limit. On the SCA claim, the court said that Arch Wireless should have been characterized as an “electronic communication service” because it enabled users to get and receive messages and, as such, is only allowed to divulge contents to the sender and receiver.

**SEARCH AND SEIZURE: SCOPE
OF SEARCH WARRANT**

US v. Giberson, 2008 WL 2221008 (9th Cir. May 30, 2008). Francis Giberson was arrested during a traffic stop after being found with false Nevada identification and without a valid driver’s license. Agents conducted a search of his residence for evidence of “ownership of assets or property” pursuant to a warrant. The agents found

materials suggesting that Giberson created false identification documents on his computer, so they got a second warrant to search it. Agents then used a “law enforcement utility software package” to organize the files on the hard drive into separate folders by type and, while searching, found images of child pornography. Giberson was arrested and later convicted of receipt and possession of child pornography in the U.S. District Court for the District of Nevada. He appealed, challenging the seizure of his computer pursuant to the first warrant and the search of the mirror image of his hard drive pursuant to the second warrant, arguing that the evidence should therefore be suppressed. The 9th Circuit Court of Appeals framed the question before the court as whether a warrant that describes particular documents authorizes the seizure of a computer where the searching agents believed that the documents specified in the warrant would be found stored in the computer. Giberson maintained that computers are technologically different from other “containers” because they store massive amounts of intangible digitally stored information, rendering them searchable only when specified in a warrant. However, the court reiterated the principle that in order to search a container, it must be reasonable to expect the items enumerated in the warrant would be contained therein. It found that the seizure of the computer was justified because the computer was reasonably believed to contain items listed in the warrant and its search was conducted pursuant to a valid second warrant. The court denied Giberson’s motion to suppress.

SEARCH AND SEIZURE:
DELAYED SEARCH OF CELL
PHONE

People v. Diaz, 81 Cal.Rptr.3d 215 (July 30, 2008). The California Court of Appeals, Second District, held that an elapsed time of approximately 90 minutes between defendant's arrest and a law enforcement officer's search of his cell phone did not render the search an invalid search incident to arrest. Gregory Diaz was arrested in his vehicle for possessing and transporting drugs. His cell phone was not searched at the time but was placed with the other evidence seized. While he was being questioned at the police station 90 minutes after the arrest, a detective accessed the text messages on Diaz' cell phone and found a message which the detective interpreted as a phrase for quantifying a drug transaction. Diaz pled not guilty, and moved to suppress the text messages. He argued that the delayed search of his cell phone violated the Fourth Amendment's requirement that a warrant be obtained for delayed searches of "possessions within an arrestee's immediate control." He further contended that cell phones should be treated differently and afforded greater constitutional protection than other items carried on one's possession because of the huge quantities of personal information they contain. The trial court denied the motion, finding the cell phone was properly searched. Diaz appealed, but the appeals court affirmed, stating that the fact that electronic devices are capable of storing vast amounts of information does not give rise to a legitimate heightened expectation of privacy. It found that a lawful custodial arrest is a "reasonable" search and an

exception to the warrant requirement under the Fourth Amendment.

Ed. Note 1: The Editor thanks Tom Clancy, Director of the National Center for Justice and the Rule of Law, for information about this case.

Ed. Note 2: The People were represented by Dave Gillette, Chief Assistant Attorney General; Pamela Hamanaka, Senior Assistant Attorney General; and Paul Roadarmel, Jr. and Victoria Wilson, Supervising Deputy Attorneys General of the Office of the Attorney General of California.

DISTRIBUTION OF CHILD
PORNOGRAPHY: SENDING
HYPERLINK

US v. Navrestad, 66 M.J. 262 (C.A.A.F. May 14, 2008). Army Specialist Joshua Navrestad allegedly transmitted a hyperlink to a Yahoo! Briefcase server containing child pornography images. He was charged with distributing and possessing child pornography. The government argued that a hyperlink to child pornography meets the statutory definition of "a visual depiction" of child pornography under the Child Pornography Prevention Act's definition, 18 U.S.C. § 2256(8). The court, however, rejected that argument, holding that a hyperlink was a shortcut to a particular Internet location, not data itself.

Ed. Note: This decision was based on a 3-2 vote. The dissent argued that "the recipient's ability to access and use images transmitted by hyperlink is functionally indistinguishable from the ability to access and use images transmitted as individually saved files."

**FIRST AMENDMENT:
DEROGATORY SCHOOL BLOG**

Doniger v. Niehoff, 2008 WL 2220680 (2nd Cir. May 29, 2008). The 2nd Circuit Court of Appeals affirmed a lower court ruling that a school district that disciplined a student for vulgar and derogatory blog posts made off campus did not violate her free speech or equal protection rights. Avery Doniger, a high school junior, was involved in planning the school's "Jamfest," when she learned school administrators were planning to postpone it. In order to prevent postponement, she posted to her LiveJournal blog calling school administrators "douchbags" and encouraging others to contact the school principal to "piss her off." Administrators found the blog, and decided that Avery should not be permitted to run for class secretary. Avery's mother as guardian and next friend sued the school district, alleging violation of Avery's first amendment rights and seeking injunctive relief of redoing the school election or giving Avery the same rights and privileges as the student who was elected secretary. The U.S. District Court for the District of Connecticut denied the preliminary injunction. On appeal, the 2nd Circuit affirmed, pointing out that had Avery's remarks occurred on campus, school administrators would clearly have been justified in disciplining her based on the U.S. Supreme Court decision in *Bethel Sch. Dist. No.403 v. Fraser*, 478 U.S. 675 (1986), which allows schools to discipline students who engage in vulgar or offensive speech. The court found that Avery's posting created a foreseeable risk of substantial disruption at the school and therefore discipline was appropriate.

**ATTEMPTED SOLICITATION OF
A MINOR: "SIGNIFICANT STEP"**

People v. Michael Z., 2008 N.Y. Slip.Op. 51400(U), 2008 WL 2746725 (N.Y. Sup. Ct. July 16, 2008). In a case of first impression, the New York Supreme Court for Nassau County found that a defendant's conduct in meeting a minor with an "instrument" to effectuate a sexual act was sufficient for a charge. The defendant in one of the Nassau County District Attorney's online predator stings appeared at the arranged meeting location, having previously told the undercover detective posing as a 15-year-old girl his intent to have sex with "her." However, the defendant passed by the meeting place twice, but never got out of his car. Police chased and arrested him after his second pass, also finding a blanket in his car. Defendant said he only had the blanket with him "to protect them from the wind and rain." However, New York, like many other states, has a "tends to effectuate" the commission of a crime statute, and the blanket was found to meet that requirement.

Ed. Note: The editor thanks Steve Treglia, Assistant District Attorney and Chief of the Technology Crime Unit at the Nassau County District Attorney's Office, for this information about his case.

E-DISCOVERY

**E-DISCOVERY: AMENDING
COMPLAINT TO ADD
SPOILIATION**

Ed Schmidt Pontiac-GMC Truck, Inc. v. DaimlerChrysler Motors Co., LLC, 538 F. Supp. 1032 (N.D. Ohio 2008). Ed Schmidt Pontiac-GM Truck ("Schmidt"), an automobile dealer, sued

DaimlerChrysler for breach of a settlement agreement. During discovery, Schmidt alleged that DaimlerChrysler failed to implement a litigation hold to prevent the destruction of evidence after the complaint was filed, and replaced or altered certain hard drives before Schmidt made forensic images of the drives as part of discovery. Further, Schmidt alleged that DaimlerChrysler sought to hide its misconduct. Schmidt moved to amend its complaint to add a spoliation of evidence claim. The U.S. District Court for the Northern District of Ohio found that Schmidt had alleged facts supporting all five elements of a spoliation claim under Ohio law, which are 1) pending or probable litigation; 2) knowledge by defendant of existing or probable litigation; 3) willful destruction of evidence by defendant; 4) disruption of plaintiff's case; and 5) damages caused by defendant's actions. However, DaimlerChrysler argued against the motion that the spoliation claim was remote from the original claim and, if allowed, would bias the jury against them. The district court rejected both arguments, finding as to the first argument that the issue of spoliation of evidence was very closely related to Schmidt's ability to prove breach. Second, the court found that adding a spoliation claim would not bias the jury any more than an adverse instruction. The motion to amend was granted.

E-DISCOVERY: SERVING SUBPOENA ON A PARTY

Thomas v. IEM, Inc., 2008 U.S. Dist. LEXIS 19186 (M.D. La. March 12, 2008). In a suit under the Family and Medical Leave Act, plaintiff Margaret Thomas served a subpoena on IEM requiring production within 15 days of

the e-mail box contents of nine supervisors and co-workers as they existed on a date two years earlier. IEM served formal objections to the subpoena on Thomas, who in turn filed a motion to compel. IEM argued that subpoenas were used for third party discovery, not discovery from another party, and also that the subpoena was overbroad and would require IEM to review 67,000 emails at a cost of 700 hours and over \$120,000. The U.S. District Court for the Middle District of Louisiana found that while Rule 45 does not preclude subpoenas to parties, it cannot be used to avoid the 30 day discovery deadline of Rules 26 and 34. Further, the court concluded that the subpoena was overbroad and did not allow sufficient time for IEM to respond, given the estimate of manpower required. The court therefore denied the motion to compel.

E-DISCOVERY: PRE-LITIGATION HOLDS

Texas v. City of Frisco, 2008 WL 828055 (E.D. Tex. March 27, 2008). The city of Frisco sent a litigation hold request to the state of Texas seeking preservation of all electronic data related to a possible environment suit. Texas moved to dismiss, arguing that the city was seeking an advisory opinion from the court on the proper method of preservation without pleading all of the elements of a viable claim. The U.S. District Court for the Eastern District of Texas agreed and granted the motion, determining that the issues were not yet ripe and urging both parties to make a good faith effort in preservation and production of documents in the absence of court intervention.

LEGISLATION UPDATE

COMPUTER FORENSICS

MICHIGAN Governor Jennifer Granholm signed H.B. 5274 into law, which makes it a felony to engage in computer forensics unless licensed as a private investigator in the state. The punishment for violation is up to four years in prison and a \$25,000 fine. Exceptions are made for attorneys licensed in Michigan and an employee acting within the scope of full time employment. The licensing requirements include three years experience, which can be comprised of a graduate degree in computer forensics or full time employment as an investigator or as an investigative reporter employed by a media outlet. The full legislation may be accessed at: <http://www.legislature.mi.gov/document/s/2007-2008/publicact/pdf/2008-PA-0146.pdf>.

SEX OFFENDERS

NEW HAMPSHIRE Governor John Lynch signed HB 1640 into law, a measure updating their Sex Offender Registry law to allow suspension of the driver's license of a sex offender who fails to register. It also divides sex offenders into three tiers based on their conduct and would allow those convicted of less serious crimes to ask a court to have their names removed from the registry list after a period of good behavior. It further compels sex offenders convicted of a number of criminal felonies to supply a DNA sample. The law goes into effect in January 2009.

CYBERBULLYING AND ELECTRONIC HARASSMENT

On July 10, **CALIFORNIA** Governor Arnold Schwarzenegger signed SB 129 into law, which extends to cellular phones and other electronic devices a law making it a crime to place phone calls with the intent to harass or annoy the recipient. The previous law removes the limitation that the calls be made to a person's workplace or home.

MISSOURI Governor Matt Blount signed SB 818 into law, amending state law against harassment by removing the requirement that harassment be written or made over the telephone. The new law makes harassment via computers, text messages or other electronic devices illegal. It also requires school boards to develop a written policy requiring schools to report harassment and stalking committed on school property to local police. While the new law continues to make violation a Class A misdemeanor, it becomes a Class D felony if 1) committed by a person 21 years of age or older against a person 17 years of age or younger, or 2) the person has previously committed the crime.

INTERNET TOBACCO SALES

VERMONT'S new law, Act 119, banning the sale of tobacco over the Internet or via telephone or mail order and shipped to anyone in Vermont other than a wholesaler or retailer, went into effect on July 1. The law also requires that tobacco vendors display at the top of all web sites a statement warning that it

is illegal for Vermont residents to buy their products.

SPAM

On July 17, **District of Columbia** Mayor Adrian Fenty signed B17-0034, the Spam Deterrence Act of 2008, into law, prohibiting unsolicited commercial e-mail, known as spam, 1) from a computer located in DC; 2) to an e-mail address of a DC resident; 3) to an e-mail service provider with equipment or its principal place of business in DC; or to a domain name registered to a DC resident. The law provides for lawsuits brought by the Attorney General, e-mail service providers and private citizens.

ONLINE CHILD EXPLOITATION

On July 7, the U.S. **Senate Judiciary Committee** approved S. 1738, a bill sponsored by Senator Joseph Biden (D-DE), requiring the establishment of an Internet Crimes Against Children Task Force under the Department of Justice that would consist of one state or local task force per state to address online child exploitation and pornography. The bill would authorize grants to the state and local task forces, as well as authorize additional forensic capability to address backlogs. It would also authorize wiretapping in state child exploitation investigations.

VIOLENT VIDEO GAMES

On July 22, **NEW YORK** Governor David Patterson signed a video game law requiring video games sold in New York to clearly label ratings for violent content. The law makes it compulsory for games that are already rated to be labeled and also requires that new video game consoles be installed with parent-controlled lockout features by 2010. It also establishes an advisory council to study “the connection between interactive media and real-life violence in minors exposed to such media” and to evaluate the ratings issued by the Entertainment Software Ratings Board.

TEXT MESSAGING WHILE DRIVING

On August 21, the **CALIFORNIA SENATE** passed SB 28, a bill that would ban text-messaging while driving and authorize a \$20 fine for violation of the law. Repeat offenders would receive a \$50 fine. The California Assembly previously passed the bill.

IP-ENABLED 911 AND E-911 SERVICES

On July 23, a bill requiring IP-enabled voice service providers to provide 911 service, including enhanced 911 (E-911) service to its subscribers, became **Public Law No. 110-283**. It mandates the development of a plan for migrating to a national IP-enabled emergency network. The legislation was sponsored by Representative Bart Gordon (D-TN).

NEWS YOU CAN USE

STUDY: EIGHTY PERCENT OF BUSINESS PCS NOT FULLY SECURED

Security firm Sophos ran 40-day Endpoint Assessment Test on 580 visiting computers from corporate users, finding that 81 percent were lacking some key security component. The test scans were voluntary and covered three areas: current patch levels, firewalls and up-to-date security software. A summary of the results showed that 63 percent of computers checked were missing at least one Microsoft security patch; 51 percent had disabled client firewalls; and 15 percent had out-of-date or disabled security software. Sophos listed some reasons for the poor showing. For example, the survey found that most people rely on Windows Update, which comes with Windows software, but it only checks for Windows patches. Users need Microsoft Update, a separate download, to check for fixes to Microsoft Office and other applications. Other reasons are: some users may decline the updates until a later time and then to update later; others disable firewalls on their PCs, thinking the corporate firewall is sufficient; and antivirus users make the same assumptions and disable their PC's security. The sample base was composed of 39 percent from North America, 36 percent from the United Kingdom, 11 percent from Australia, nine percent from Germany and the remaining five percent from several countries.

COMPANIES RELUCTANT TO FARM OUT DATA ARCHIVING

Only 24 percent of companies are using hosted data archiving, compared with 76 percent using on-premise technologies, according to a study by the Radicati Group, a research firm. The reason, according to Radicati, is that companies are fearful of missing data or of their inability to retrieve the data in response to a government request. Another concern is that data could be more easily compromised when stored offsite. Radicati said that this reluctance to adopt a Software as a Service (SaaS) model continues even though hosted archiving is cheaper and easier to deploy. Nevertheless, this slow adoption rate is expected to change, since the SaaS industry is experiencing a 300-400 percent growth each year, and the Radicati Group predicts it will grow to \$2.7 billion by 2012.

STUDY: ONLINE GAMBLING SHOULD BE LEGALIZED

The United States and Canada should legalize and regulate online gambling because players tend to bet more frequently and aggressively than they do in casinos, according to a study conducted jointly by the University of Nevada in Las Vegas and the University of Western Ontario in Canada. The study found that online gambling is readily accessible on the Internet, even though it is banned or in a "legal grey area" in the two countries. It is big business, and the study estimated worldwide spending at more than \$10 billion a year. The study found that betting online is a problem because it has the potential to be more addictive than casino gambling. Online gamblers can hide their activity more easily, and betting can quickly

become a routine part of daily lives. The study's authors suggest that governments encourage large corporations like those that run the major Las Vegas casinos to enter a regulated online gambling market as one potential solution.

REPORT: CYBER-CRIMINALS RESPONDING QUICKER TO FLAWS

Criminals on the Internet are narrowing the time it takes to unleash computer attacks that take advantage of publicly disclosed security holes, according to IBM's latest Internet Security Systems X-Force report. The report looked at the first six months of 2008 and reflects two growing trends in Internet threats. The first trend is that online criminals are now using programs that help them automatically generate attacks based on publicly available information about vulnerabilities. In the past they spent more time finding those security holes themselves, but find it is no longer necessary. The second trend is that the debate is intensifying among security researchers over how much information should be released publicly when a new software flaw is found. Although usually researchers will wait until the affected company has released a software patch before revealing details, sometimes they will release not only details of the vulnerability but also "proof-of-concept" exploit code to show the flaw is legitimate. That practice provides criminals a framework for building their attacks. In web browsers, hacking exploits were available within one day after flaws were discovered 94 percent of the time, up from 79 percent in 2007, according to the report. For PC vulnerabilities, over 80 percent of the code was released the same day the security holes were disclosed, up from 70 percent last year. The report also found that spammers are changing tactics by shifting away from pictures and complicated messages to simple messages and a sole web link to evade spam

filters and redirect users to web sites under their control. The full report can be accessed at <http://www-935.ibm.com/services/us/iss/xforce/midyearreport/>.

PROJECT TO REBUILD INTERNET GETS \$12 MILLION FUNDING

The Global Environment for Network Innovations (GENI), a massive project to redesign and rebuild the Internet from scratch, received \$12 million in grants from the National Science Foundation to develop prototypes for GENI. Many researchers want to rethink the Internet's underlying architecture, saying a "clean slate" approach would address security and other challenges that have arisen. BBN Technologies Inc. is overseeing the planning and design of GENI, on which researchers will be able to test new ideas without damaging the current Internet. Additionally, the Internet2 organization is contributing 10 gigabits per second of dedicated bandwidth, so normal Internet traffic will not interfere with experiments. National LambdaRail is offering another 30 gigabits per second of capacity, although it won't be dedicated at all times. Construction on GENI could start in five years and cost \$350 million, although Congress still has to approve those funds.

NEW LAPTOP BAGS MAY STOP AIRPORT HASSLE

The Transportation Security Agency (TSA) gave luggage manufacturers the green light to produce new bags that would allow laptops to go through security without being removed from the bag. Currently, the laptops must be removed because items such as power cords and mice may prevent proper screening. Prototypes of the bags are now being tested at three airports, and manufacturers such as Targus and Pathfinder say the bags will be available in early fall. While the TSA will not

rubber-stamp the bags, manufacturers will be allowed to place a “checkpoint friendly” tag on them.

ANTI-SPAM GROUP ISSUES GUIDELINES FOR ISPS

The Messaging Anti-Abuse Working Group (MAAWG), a global anti-spam organization, issued guidelines for ISPs to enable them to block spam e-mail without blocking users who forward their e-mail from one account to another. MAAWG recommends separating the servers that received e-mail from servers that forward e-mail to fix that problem. The guidelines also address the problem of computers sending spam after being infected with malicious software. MAAWG suggests that ISPs block the dynamic IP addresses, or share information about dynamic addresses if they cannot be blocked. The recommendations on dynamic IP addresses can be accessed at http://www.maawg.org/about/publishedDocuments/MAAWG_Dynamic_Space_2008-06.pdf. The recommendations about e-mail sharing can be accessed at http://www.maawg.org/about/publishedDocuments/MAAWG_Email_Forwarding_BP.pdf.

REPORT: BOTNET SPAM FIGHT IS HOPELESS

CommTouch, an anti-spam company, released its quarterly report detailing what it calls the “hopeless” battle against botnet spam. The company uses a “zombie monitor” to track botnets and other spam. According to the report, by the time computers are identified as infected with botnets, the investigation is futile because the botnet has already moved to other computers. The report also details that the U.S. is ninth on the list of the countries sending the most spam. Turkey, Brazil, Russia, Italy and India are the top five. The full report may be accessed at

http://www.commtouch.com/documents/CommTouch_Q208_Email_Trends.pdf.

REPORT COMPARES CYBERCRIME TO ORGANIZED CRIME

Security firm Finjan released its second quarter Web Security Trends Report, which likened cybercrime to organized crime. The report explains that the current structure of cybercrime has evolved from a few hackers working together into a hierarchical organization, such as the mafia, where there is a “boss” directing the organization. Other players in the hierarchy include seconds in command who organize and plan the attacks, “soldiers” who steal the data and “resellers” who trade the stolen data. The report notes that cybercrime is not limited to attacks, but has expanded to include “one stop Crimeware shops,” where hackers sell toolkits to other hackers who are less technology-oriented. The full report can be accessed at <http://www.finjan.com/Form.aspx?id=678&Openform=true&ObjID=620>.

CYBERSECURITY TO BE LARGE PART OF 2009 BUDGET

The U.S. House Select Committee on Intelligence issued a report that revealed the largest part of the new budget would be allocated to the Comprehensive National Cybersecurity Initiative. While there are few details available about the program, its purpose is to secure government computer systems against intrusions, prepare for future threats and secure vital infrastructure data. The committee recommended that another committee composed of lawmakers, executive branch officials and private sector representatives should oversee its implementation. The committee report on the cybersecurity bill can be accessed at http://intelligence.house.gov/Media/PDFS/IA_AFY09.pdf.

HOUSE COMMITTEE PROBES INTERNET TRACKING

The U.S. House Energy and Commerce Committee sent letters to more than 30 telecommunications and Internet companies, demanding to know whether they track where their users go online and use that information to deliver personalized advertising. Among the companies receiving letters were Google Inc., Yahoo Inc., Microsoft Corp., AT&T Inc., Comcast Corp., Quest Communications International Inc., Verizon Communications Inc., Time Warner's AOL unit and Time Warner Cable Inc. All were given one week to respond. The letters seek details on the number of consumers tracked, whether those consumers were notified and whether they were given a choice to "opt out." The committee also wants details on how the information is collected and how it is used.

POLL: E-DATA BECOMING UNMANAGEABLE

Nearly 40 percent of executives feel that data volumes in their organizations are increasing and becoming unmanageable, according to an online poll of executives conducted by Deloitte Financial Advisory Services. At issue for most is a Federal Rules of Civil Procedure amendment requiring companies to have the ability to quickly access electronically stored information in the event of litigation. The poll showed 17.5 percent of executives feel that their companies are not ready to handle complex discovery requests. Nearly 12 percent of companies polled have no policy providing clear guidance for the IT department and other employees on document retention and destruction. The greatest concern expressed was the expense of reviewing large volumes of files, in addition to liability for errors and failure to meet deadlines set by the courts. The poll covered 520 executives from banking, securities, financial services and technology and was part of a webcast called "Strategic Discovery: Taking Steps to Avoid Litigation's Black Hole."

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

COMPUTER CRIME IN THE WIRELESS AGE

**October 21-23, 2008
University, MS 38677**

NOMINATION FORM - RETURN BY SETEMPBER 29, 2008

****PLEASE NOTE: THIS FORM IS NOT AN AUTOMATIC APPROVAL TO ATTEND THE TRAINING.
APPROVAL NOTICE WILL BE SENT UNDER SEPARATE COVER****

MEETING ID NO. # 0810_CYBWA

Please use one form per registrant/nominee. Complete *all* sections.

Please return form to: National Association of Attorneys General, Attn: Marland Holloway, Cybercrime Project Assistant, 2030 M Street, N.W., 8th Floor, Washington, DC 20036 or **Fax to (202) 331-1427.**

Name (as it should appear on badge): _____	Full Mailing Address: _____
Title: _____	_____
Phone Number: _____	_____
Fax Number: _____	
E-mail: _____	
Attorney General Office: _____	

Travel By (Check one): Air Rail Car

**State Bar registration number(s)
(For CLE credit)**

State _____ Number _____

State _____ Number _____

Dietary Restrictions? If so describe: _____

Special Requests If you require special services or auxiliary aids to assist you while attending the meeting and events during the Cyber Crime Training, such as sign-language interpreters, note-takers, large print materials or Braille materials, please contact Marland Holloway, Cyber Crime Project Assistant, at 202-326-6262 or by email at mholloway@naag.org. NAAG will make suitable arrangements.

(NAAG Use Only):

This Nominee Has Been Approved To Attend This Training: Yes () No ()