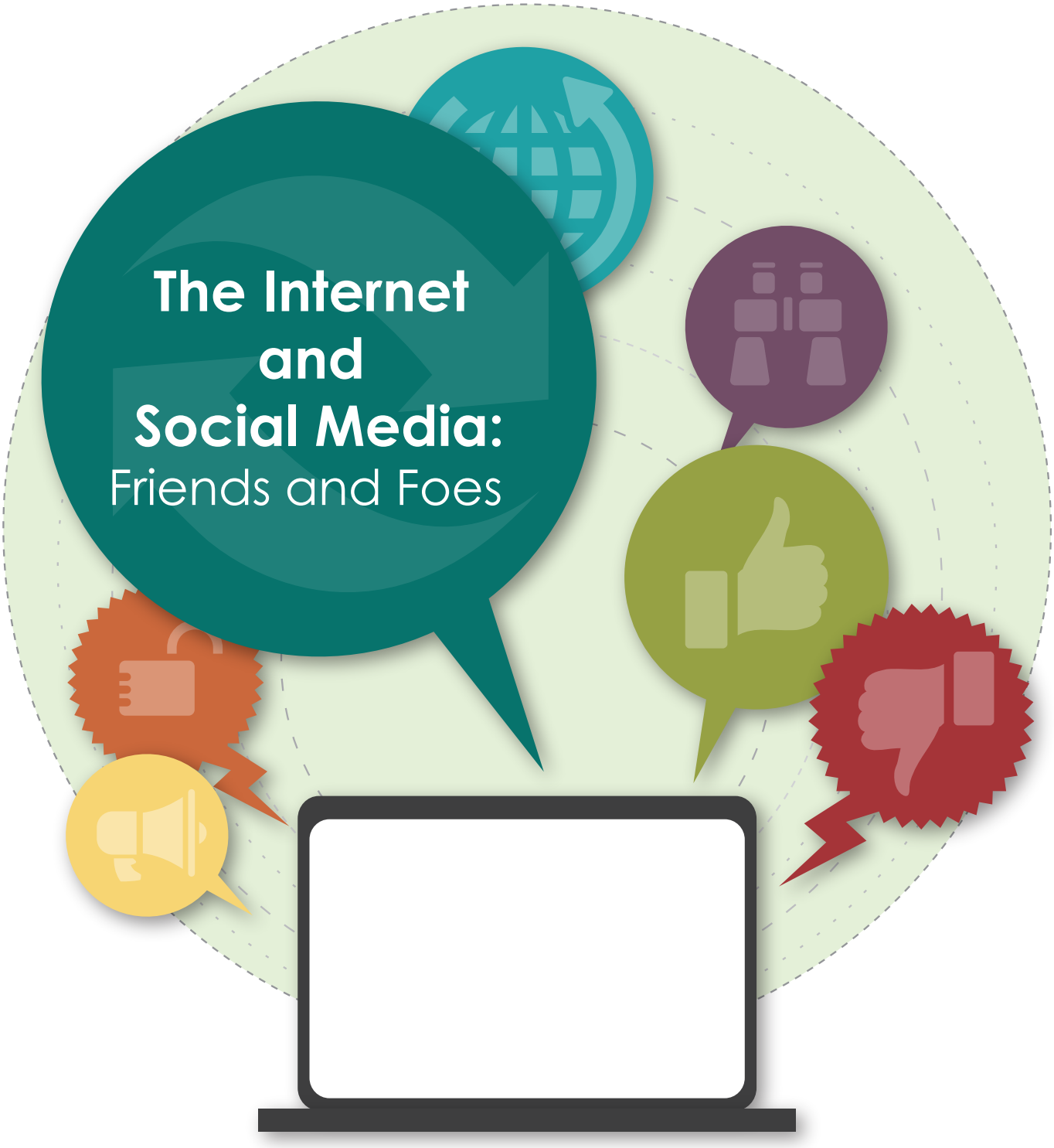
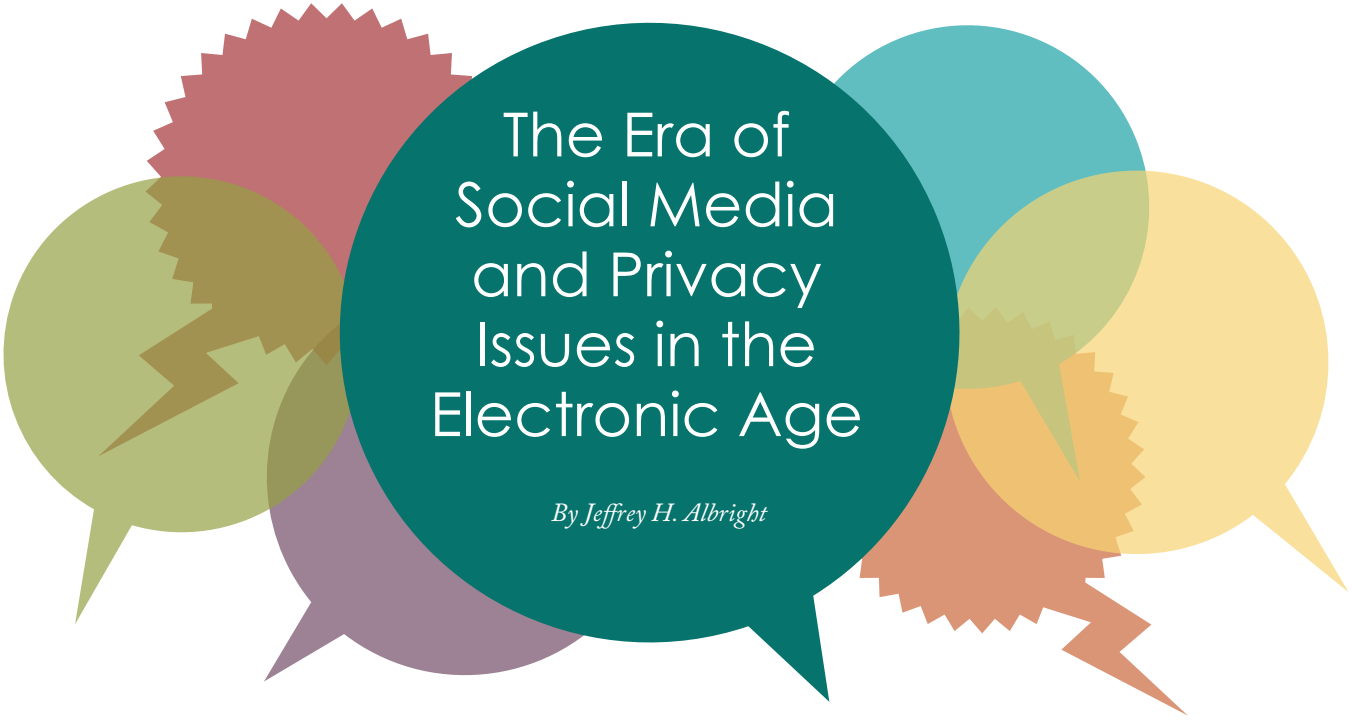
NEW MEXICO
Lawyer
February 2013 Volume 8, No. 1 www.nmbar.org



State Bar Intellectual Property Law Section



The Era of Social Media and Privacy Issues in the Electronic Age

By Jeffrey H. Albright

At home or in the office, during work or at play, with our peers and colleagues or with family and friends, we have become increasingly connected via social media. Broadly speaking, the definition of "social media" is any technology that lets people publish, converse and share content online. As of Dec. 2, 2012, Wikipedia listed more than 200 active social media websites, from sites such as Facebook with 908 million subscribers to NGO Post (in India) with 15,000 subscribers to The Sphere, a "private online social luxury network with exclusive personalized services," with 1300 members.[1] Although there is a common perception that social media is limited to a specific generation, a recent study by the Houston Chronicle stated that 69 percent of online adults, including 38 percent of Americans over the age of 65, use social media. It affects everyone.[2]

> ... 69 percent of online adults, including 38 percent of Americans over the age of 65, use social media.

In addition to the broad appeal of networks in the social context, social networks have broad application to the workplace. Recent surveys indicate that 88 percent of companies survey or consider social media as part of their hiring process. Additionally, more employers are creating social media policies in the workplace.[3]

This issue of the *New Mexico Lawyer* focuses on the inherent legal conflicts that arise between privacy issues and the broad use of electronic media.

Gina Constant describes various discovery-and privacy-related issues that arise in the context of litigation.

In a related article, Ian Bezpalko highlights ongoing state legislation and federal legislation of the Social Online Protection Act under the Stored Communications Act and the Computer Fraud and Abuse Act to provide additional privacy rights for individuals.

Talia Kosh, 2013 chair of the Intellectual Property Law Section, analyzes the benefits and potential impact of social media "crowdfunding" on film makers, start-ups, and small businesses and the impact of the federal Jumpstart Our Business Startups Act on the filmmaking industry.

As we sign up for social media and establish various electronic accounts, the laborious reading of terms of service agreements when acquiring new products and enrolling in various programs is critical but often overlooked and even avoided by most people as they click on "accept" without reading terms and conditions. Using two recent case studies, Peter Ives identifies some of the help available to those for whom the review of such agreements is too taxing or incomprehensible. Ives also highlights some of the provisions that should serve as warnings before a person accepts the privacy issues and terms of service agreements.

Finally, I provide some "best practices" for creating strong password protections that should be considered by every individual, regardless of the frequency or extent of one's use of social media or the Internet.

Endnotes

[1] "List of Social Networking Websites," http://en.wikipedia.org/wiki/List_of_Social_networking_websites.

[2] *Houston Chronicle*, "The List: 11 Social Media Trends of Importance to Political Junkies," Sunday, Dec. 2, 2012

[3] *National Law Journal*, Nov. 28, 2012.

Scope of Discovery of Social Networking Website Content

By Gina T. Constant

A typical claim for personal injury includes physical injuries as well as emotional distress and loss of enjoyment of life. Sometimes, and perhaps more often than not, the plaintiff's social networking website accounts will be mined by defense counsel for relevant content. For instance, did a plaintiff who claims to have been so seriously injured in an auto accident that she can barely walk actually go snow skiing last weekend and post pictures on Facebook?

... how do courts address a request for a plaintiff's social networking site content?

So how do courts address a request for a plaintiff's social networking site (SNS) content? While there is not an abundance of case law on the topic, some general themes are emerging.

Courts addressing this issue have attempted to balance privacy concerns with liberal discovery rules. The privacy rights are usually based on three sources: The Fourth Amendment, Title II of The Electronic Communications Privacy Act, and Rule 26(c)(1) of the Federal Rules of Civil Procedure. The protection afforded by these sources varies. First, the Fourth Amendment will not support a claim of privacy since there cannot seriously be a reasonable expectation of privacy when a person took the affirmative action of posting content and opening it up to the public eye. *Romano v Steelcase Inc.*, 907 N.Y.S.2d 650, 654 (N.Y. Sup. Ct. 2010). Also, SNSs like Facebook and MySpace have disclaimers that preclude a poster from having a realistic expectation of privacy, which is a requirement for Fourth Amendment protection. Second, Title II of the Electronic Communications Privacy Act prohibits SNSs from disclosing a customer's electronic communications without the customer's approval. 18 U.S.C. §§ 2701, 2702. And a subpoena to the SNS in a civil action is no exception to the Act. 18 U.S.C. § 2702(b); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 609 -611 (E.D. Va. 2008). Finally, parties who resist providing their SNS content in discovery usually seek a protective order pursuant to Rule 26(c)(1), which allows such "an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden."[1]

To overcome these privacy protections, the party seeking the SNS content must show that the requested SNS content is relevant to a claim or defense in the case and the request must be narrowly tailored enough so that it is reasonably calculated to lead to the discovery of admissible evidence. *Mailhoit v. Home Depot U.S.A., Inc.*, No. 11-3892, 2012 U.S. Dist. LEXIS 131095, at *7-*9 (C.D. Cal. Sept. 7, 2012).

The following are some examples of how courts have balanced the competing interests of privacy and liberal discovery:

- Where the plaintiff alleged serious physical injuries, emotional distress, and impaired quality of life, the court required the plaintiff to upload onto an electronic storage device SNS information within a relevant timeframe.[2] The device was to be delivered to defense counsel who was required to keep the information confidential. The parties could then come back to court if disputes remained.

- In another case, the defendant served very narrow discovery requests asking only for SNS content specifically related to the plaintiff's allegations of "teasing and taunting."[3] An *in camera* review by the court showed that the plaintiff's production was so under-inclusive that the court required her complete SNS profile be provided to the defendant.

- Another court in a dispute about the scope of discovery of photographs on a party's SNS pages gave the parties the following guidelines:

> [P]ictures of the claimant taken during the relevant time period and posted on a claimant's profile will generally be discoverable because the context of the picture and the claimant's appearance may reveal the claimant's emotional or mental status. On the other hand, a picture posted on a third party's profile in which a claimant is merely 'tagged,' is less likely to be relevant. In general, a picture or video depicting someone other than the claimant is unlikely to [be relevant].[4]

- Closer to home, a plaintiff in our federal district court alleged sexual harassment and emotional damages and testified in her deposition that her depression included a loss of interest in socializing and dating.[5] Therefore, social networking was squarely before the court and access to her social networking sites was deemed to be relevant. First, in order to avoid the release of the plaintiff's password and login information, the court ordered the parties to meet at the plaintiff's attorney's office so that the plaintiff could open her Facebook, Twitter, and MySpace pages. When the court determined that there was evidence that the plaintiff may have deleted her MySpace account while the lawsuit was pending, it ordered her to provide defense counsel with written consent to a subpoena to MySpace for all stored content.

So attorneys should feel free to request relevant SNS content. Also, attorneys should know that they will not be sanctioned for secretly perusing an opposing party's public content unless they used improper means to hack into the account. *Womack v. Yeoman*, 2011 Va. Cir. LEXIS 143 at **2-**5 (Va. Cir. Ct. Oct. 28, 2011). Finally, attorneys would be wise to advise their clients to make their Facebook, Twitter, MySpace, LinkedIn, and other SNS profiles "private" as soon as litigation is anticipated, but know that private SNS content is not immune to discovery if the previously public content suggests discoverable information in the now-private content. *Romano,* 907 N.Y.S.2d at 656.

Endnotes

[1] New Mexico's rule contains the same language. *See* Rule 1-026(C)(1) NMRA.

[2] *Thompson v. Autoliv ASP, Inc.*, No. 09-1375, 2012 U.S. Dist. LEXIS 85143, at *13-*15 (D. Nev. June 20, 2012).

[3] *Bass v. Miss Porter's School*, No. 08-1807, 2009 U.S. Dist. LEXIS 99916 at *1 (D.Conn. 2009).

[4] *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 436 (S.D. Ind. 2010) (footnote omitted).

[5] *EEOC v. Genesco*, No. 09-952, Mem. Op. & Order (D.N.M. Feb. 15, 2011).

Gina Constant is a registered patent attorney at the Rodey Law Firm in Albuquerque. In addition to her legal experience, she has 20 years of business experience including two years as a process engineer at a nuclear-chemical processing plant, fourteen years as an engineer and manager at Intel, and five years in partnership with her husband running a small health care business.

Privacy *and* Social Media

By Ian Bezpalko

An article by Marc Andreesen in the Aug. 20, 2013, edition of the *Wall Street Journal* stated outright that "software is eating the world." By this, Andreesen meant that software is superseding hardware in importance—if only because hardware has been outsourced—and that Internet companies such as Facebook and Twitter represent the future of what we call computing. Through such applications, anybody can build a personal brand and leverage it in employment interviews. We in the legal profession can see a fundamental shift in the way companies recruit and retain employees. With this shift new issues arise that business must address, particularly in the areas of privacy and confidentiality. Unfortunately, the dominant approach appears to be to shoehorn fixes into the current framework.

Some states are moving to block employers from asking for access to online profiles.

Facebook's Statement of Rights and Responsibilities, last revised June 8, 2012, states clearly under paragraph 4, point 8, that a subscriber "will not share [their] password … let anyone else access [their] account, or do anything else that might jeopardize the security of [their] account." Facebook itself cautions that by accessing a Facebook page, an employer may find that the employee is a member of a protected group and thus the employer may be liable to a claim of discrimination if the potential employee is not hired.[1]

Some states are moving to block employers from asking for access to online profiles. Illinois Governor Pat Quinn signed such a law[2], which even prevents the request for such information regardless of whether the employer must conduct a thorough background check. Maryland, the first state to pass a law preventing employers from requesting or requiring that an employee surrender login details, codified the law at Ann. Code. Md. §3-712 (2008 Replacement Volume and 2011 Supplemental), which took effect Oct. 1, 2012. Comparatively, it does not go as far as the Illinois law and permits the access of online accounts to ensure compliance with applicable securities or financial law, or regulatory requirements. New Jersey and California are considering similar legislation.

Also attracting attention are two current federal laws, the Stored Communications Act and the Computer Fraud and Abuse Act. The SCA, 18 U.S.C. § 2701, prohibits intentional access to electronic information without authorization or by intentionally exceeding limited authorization, and the CFAA prohibits intentional access of a computer, without authorization, to obtain information under 18 U.S.C. § 1030(a)(2)(C). Civil liability under the SCA has been found when a company requested an employee's login credentials in order to access private information contained in a chat group (*Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 (D.N.J. 2009)), and on an employee website (*Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002)).

New federal legislation to address privacy concerns and make it an offense to request login credentials as part of an employment application has been proposed. On April 27, 2012, Representatives Eliot Engel and Jan Schakowsky introduced H.R. 5684, the Social Networking Online Protection Act. Currently, the bill is before the House Committee on Education and the Workforce. On May 9, 2012, Senator Richard Blumenthal introduced as companion legislation the Password Protection Act of 2012, Senate Bill 3074. The bill is currently before the Senate Committee on Health, Education, Labor, and Pensions.

Future employees and current ones will certainly use the services of Facebook, Twitter, and other online applications to build a brand. In doing so, no one should ignore ramifications of this endeavor, including the inevitable surrender of one's privacy.

Endnotes

[1] http://www.facebook.com/note.php?note_id=326598317390057.

[2] H.B. 3782, amending Section 10 of the Illinois Right to Privacy in the Workplace Act, (820 ILCS 55), into law. See P.A. 097-807.

Ian Bezpalko is a member of the Intellectual Property Law Section and and has been in private practice for six years.

The US JOBS Act and Crowdfunding:

Will It Be a "Game Changer" for Filmmakers, Start-ups and Small Businesses?

By Talia Kosh

On April 5, 2012, President Barack Obama signed the Jumpstart Our Business Startups Act (JOBS Act) into law to spur job creation by small companies and start-ups by relaxing the regulatory burdens of raising capital.

The JOBS Act allows small businesses and creative companies to access funds outside of the large accredited investor or venture capital firm. Specifically, it amends the Securities Act of 1933 with a registration exemption for transactions involving individual investments limited to the lesser of $10,000 or 10 percent of an investor's income. Additionally, the entrepreneur can raise up to $1 million within a 12-month period through an SEC-registered "crowdinvesting portal." The prediction is that the JOBS Act will change the face of venture capitalism. Only time will tell whether it will truly result in a new version of the American dream.

It is clear there is a great need for the JOBS Act. Small and mid-cap companies have been few and far between in the public-funding game for many years, and entrepreneurs are facing a global capital crunch along with fewer banks offering small business loans. The JOBS Act is an attempt to ease the problems of attracting capital in a difficult market.

Current crowdfunding regulations only allow offerings of non-monetary, donation-based rewards to donors and prohibit offering a stake in the company or a percentage of the profits. Many crowdfunding sites have already shut down because they cannot pursue helpful innovations due to such limitations. The JOBS Act has asked the SEC to adapt these rules to the current economy and the rapidly changing digital age.

When these new rules are written and adopted by the SEC by 2014, the regulatory landscape could be a "game changer" for the start-up and creative company. Creative companies and filmmakers around the nation await the SEC's rules with a hopeful eye. The SEC's interpretation of the bill and its amendments will determine to what degree this landscape will truly change. However, the JOBS Act was strongly opposed by the SEC and state securities regulators, and it will be years before everyone will be able to comprehend all of the opportunities, limitations, and areas for potential fraud.

With the JOBS Act's "crowdfunding exemption," the latest type of crowdfunding opening up new territory in raising money and soliciting investment, is equity-based crowdfunding, also known as "crowdinvesting." Rather than crowdfunders merely receiving a perk for their donation, such as a letter of acknowledgement for a limited edition DVD, funders may become shareholders of the company with their contributions, receiving returns if the company does well.[1]

> Crowdfunding's capacity for networking and the ability to create a fan base for a company or its product is unrivaled.

Since the passage of the JOBS Act, we have seen ever-increasing usage of crowdfunding platforms such as Kickstarter, Indiegogo and Fundable. These crowdfunding platforms have helped fund everything from startups to film and music projects to product ideas. While the forecast is still unclear as to the long-term viability of these platforms, crowdfunding should be a consideration for any start-up or creative company.

The SEC's interpretation of the JOBS Act may be disappointing to many. Some are predicting that the SEC will lean toward requiring that registered broker-dealers be involved in each crowdfunded transaction. If regulated equity crowdfunding requires a

continued on page 10

Patent Law to Change Dramatically March 16

What You and Your Client Need to Know About the America Invents Act (AIA)

By Diane Albert, PhD, Licensed Patent Attorney

The patent law change going into effect on March 16, 2013, has immediate impact anyone who is thinking about protection for any invention s/he has created in the past.

HR 1249, the Leahy-Smith America Invents Act (AIA) shifts the United States from a "first-to-invent" system to a "first-to-file" system. If any of your clients has been sitting on an invention for years, even decades, and has the proof via lab notebooks that s/he is the first to invent, they need to act now to file a patent application!

There is much at stake for inventors and prospective inventors, and it is important to direct your clients to experienced patent attorneys who know how to help entrepreneurs to successfully navigate the changes and plan for future protection. Small companies and independent inventors in particular need to talk to an IP attorney to help them create a strategy to win the day in the "race to file."

Six-month grace period ends March 16

The AIA (also called the Patent Reform Act of 2011), enacted on September 16, 2011, changes the rules. After March 15, 2013, a claimed invention is not novel if it:

> "was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention"

or:

> "was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention."

Major points regarding the First-Inventor-to-File are the applicant must be the true inventor or assignee; the "effective filing date" equals the earliest priority date; prior art is expanded to include disclosure available to the public anywhere; "effectively filed" includes foreign priority dates; and the priority date will be the effective date for both novelty-defeating and obviousness.

Exceptions to prior art include a one-year grace period for inventor or joint inventor which applies to all "disclosures" which may include offers, sales and public uses.

Other areas of change in AIA

There are three other major areas of change that may affect your clients:

- Patent Office prosecution fees and funding
- Litigation reforms
- Patent Office proceedings

Act now!

Whether your clients believe they have something patentable, are considering filing a patent in the future, or have protected IP in their business or their business plans, they need to evaluate their situation in light of the AIA. Changes in policies and proceedings can mean delay or disappointment if an inventor does not understand the new landscape. Any client who is depending on patent protection for successful execution of his/her business strategy needs to talk to an experienced, dedicated patent attorney now.

Like this type of information?

Albuquerque Business Law's IP Division is here when you need us to provide IP protection and litigation expertise. For regular updates in IP law and how it affects you and your clients, subscribe to our blog at **www.albuquerquebusinesslaw.com/blog.**

ALBUQUERQUE BUSINESS LAW, P.C.
INTELLECTUAL PROPERTY DIVISION

The US JOBS Act and Crowdfunding *continued from page 7*

broker-dealer with higher fees and revenue expectations, this will make it more difficult for small businesses to benefit from these deals and, consequently, from the JOBS Act. As crowfunding portals are intended to be an alternative to broker-dealers, it will be hard to watch broker-dealers taking away most of their business should these rules be written as some are predicting.

More disappointing is the SEC's answers to some preliminary questions about investor accreditation requirements. The SEC stated that different investors may need to supply the government with different information based on the type of investor they are considered. [2] This suggests rules which will be even more difficult for creative companies to understand, as now investor accreditation may change depending on how that investor is solicited.

Yet there is still much room for optimism. On Kickstarter last year, 10,000 different projects raised nearly $100 million combined, and over one million people have financially contributed. A culture is developing around crowdfunding and the opportunities are increasing, even extending to the manufacturing sector with 3D printing technologies that could allow people around the world to build and sell their own creations, with just a small injection of capital from the "crowd."

Whatever way the SEC writes the rules, crowdfunding still has the spotlight. Crowdfunding's capacity for networking and the ability to create a fan base for a company or its product is unrivaled. Reaching high numbers of smaller investors, who have an even wider reach of their own contacts, can have potentially greater value than working with a few large private investors. This can make everyone in the crowd "friends" who can come together and make real investments in companies they believe in. Investment then becomes a game of how to build community support and engagement at all phases of a business. As Sam Hogg at entrepreneur.com has stated, "Equity crowdfunding has essentially created a new era, that of the recreational venture capitalist."[3]

The SEC is still taking public comments on their rulemaking for JOBS Act provisions at www.sec.gov/spotlight/jobsactcomments.shtml. Please reach out to the SEC and let them know your thoughts and how this legislation might impact your clients.

Endnotes

[1] Sec.gov, "US JOBS Act, Frequently Asked Questions."

[2] Jason Best, "SEC uses JOBS Act to Set up New Roadblocks to Crowfunding," Venturebeat.com, August 31, 2012.

[3] Hogg, Sam, " JOBS Act Legislation Opens Up Crowfunding," Entrepreneur,com, September 28, 2012.

Talia Kosh is an associate at The Bennett Firm in Santa Fe, practicing in the areas of employment law, personal injury, contract law, nonprofit matters and copyright law. She is the president and founder of New Mexico Lawyers for the Arts, a nonprofit organization providing pro bono legal assistance and educational programs to artists and art organizations.

Privacy Issues in the Electronic Age: Terms of Service Agreements

Subtitle: It was too long; everyone has to accept it; I just wanted the program; I didn't have time; it was all in legalese; the dog ate my homework and other excuses.

By Peter Ives

Terms of service agreements are everywhere you look in this electronic age. Every time you sign up online for a new account, you are generally compelled to "<click>" to accept the terms and conditions under which the provider of the account or software is willing to provide the service. These agreements are drafted long before you, the consumer, are ever involved in your part of the transaction, and so there is never an opportunity for you to negotiate those terms. Such terms of service agreements, while occasionally written in plain English, often contain provisions that only a lawyer who has studied contracts will grasp or understand. These agreements are generally binding (that, however, is a topic for another day), and certainly it is best to presume that if push comes to shove, you will need to abide by those terms. After all, nobody made you set up that account or buy that software. This sin of omission, signing an agreement we have not read, is one we are all likely guilty of, especially when the new version of a particular software is out, perhaps ITunes 11.0, and we signed up back when it was version 8.2.

So you ask, "How bad can that be?"

Wow! That's Amazing!

So you ask, "How bad can that be?" The answer (not surprising given what can be done via our computers in this day and age) is that it can be very bad. A recent proceeding before the Federal Trade Commission, *In the Matter of Designerware, LLC, et al.*,[1] is illustrative of the extent to which modern technology can be used inappropriately. Earlier this year, the FTC filed a complaint which contained some rather startling allegations. To understand the nature of the allegations, the business operation must be understood.

Designerware created PC Rental Agent, a software package marketed to rent-to-own stores, especially those renting electronic equipment such as computers. Most often, a consumer, without sufficient funds to buy outright or credit to finance the acquisition through other means, signs an agreement to rent the computer with an option to purchase for a fixed price after paying some amount as rent. The product was a hit in the rent-to-own industry.

"As of August 2011, approximately 1,617 rent-to-own stores in the United States, Canada, and Australia ha[d] licensed PC Rental Agent. PC Rental Agent has been installed on approximately 420,000 computers worldwide."[2]

A portion of the PC Rental Agent software involved an application or module entitled "Detective Mode," which allowed a user to not only track the physical location of the computer, but also to record data entered into the computer by the lessee. It even allowed the rent-to-own company to see the consumer surreptitiously through the computer's webcam. Beyond that, Detective Mode allowed the company "to cause fake software registration windows to pop up on rented computers and gather consumer's personal information."[3] No requirements existed for rent-to-own companies to advise their lessees that these features were on the machines, and "[t]he presence of PC Rental Agent [was] not detectable to a computer's user and the computer's renter cannot uninstall it."

The FTC noted:

> "in numerous instances, data gathered by Detective Mode has revealed private, confidential, and personal details about the computer user. For example, keystroke logs have displayed usernames and passwords for access to email accounts, social media websites, and financial institutions. Screenshots have captured additional confidential and personal information, including medical records, private emails to doctors, employment applications

> containing Social Security numbers, bank and credit card statements, and discussions of defense strategies in a pending lawsuit…. In numerous instances, Detective Mode webcam activations have taken pictures of children, individuals not fully clothed, and couples engaged in sexual activities."

Makes one think "Wow! That's amazing!" and pretty scary. The opportunity for gathering information about you is vast and not to be underestimated. What can be legally collected is often a matter set forth in terms of service agreements as well as in various statutes. In the Designerware Case, the draft consent order prohibited:

> "[l]icensing, selling, or otherwise providing any third party with geophysical location tracking technology for installation or activation on a computer to be rented in a covered rent-to-own transaction, without requiring as a condition of the license, sale, or other provision of the technology that the third party obtain consent and provide notice as provided. . .above."[4]

What was set forth above were requirements for clear and prominent notice regarding geophysical tracking technology; receipt of an express affirmative consent by the computer user to same; and an icon that, when clicked, would indicate whether the geophysical tracking was on or not.

Statutes also put parameters on use of such information gathered by computer program and software providers. There are a host of such statutes, but one which was recently seen in litigation was Michigan's Video Rental Privacy Act.[5] In *Deacon v. Pandora Media, Inc.*, 2012 WL 4497796 (N.D. Cal.; Sept. 28, 2012) the court was asked to determine whether a class action suit could be maintained against Pandora Media, Inc. Pandora is an Internet custom radio station service provider. Through its website, www.pandora.com, subscribers to the service can, in effect, create their own radio station by simply entering the name of a particular song or artist. Once the preference is expressed, Pandora streams music from the same artist or songs with similar attributes. To enable Pandora to stream music, a subscriber must sign up on the Internet and provide certain information, including name and profile information, which is loaded onto a "Personal Page," which with use contains certain additional information including recent "station" selection, recent activity, listening history, bookmarked tracks, and bookmarked artists. In April 2010, Pandora "unilaterally integrated its subscribers' profile pages with their Facebook accounts." (citation omitted.) As a result, a Pandora subscriber's Facebook "friends" allegedly are now able to access "sensitive listening records" and "musical preferences" from the Pandora subscriber's profile."[6] The VRPA provides, in pertinent part, that:

> "a person, … engaged in the business of selling at retail, renting, or lending … sound recordings … shall not disclose to any person, other than the customer, a record or information concerning the purchase, lease, rental, or borrowing of those materials by a customer that indicates the identity of the customer." *Id.*, p.6.

The plaintiff alleged that Pandora violated the provisions of the VRPA by disclosing the Pandora customer's name and listening history. The district court dismissed the plaintiff's complaint, noting in part that

> Plaintiff also fails to confront the fact that Pandora's Terms of Use, which govern a subscriber's use of the Pandora internet radio service, foreclose any borrowing or use of any temporary song file supplied by Pandora. . . . In particular, the Terms of Use plainly states[sic] that subscribers shall not "copy, store, edit, change, prepare any derivative work of or alter in any way any of the tracks streamed through the Pandora Services. *Id.*, pp.9-10.

The terms of service agreement, upon which provision of the service by Pandora was based, allowed Pandora to successfully argue that its users were not "borrowing" any music, one leg of a possible violation of the VRPA. While the disclosure of a person's music listening preferences might not seem of extraordinary importance, a minimal $5,000 penalty across the class of Pandora subscribers made for a large potential damage award.

What to do? One option is to actually print and read through the terms of service agreement each time the issue arises. That way, at least, you will know from an informed perspective what is being done to you or what is being done with your information. That would be a best practice. If the thought of that is still too onerous to contemplate, you might try using one of the helpful websites out there that does the bulk of that heavy lifting for you, such as Terms of Service–Didn't Read (http://tos-dr.info/), a crowd-sourced site that evaluates terms of service agreements, noting, "We are a user rights initiative to rate and label website terms & privacy policies, from very good 'Class A' to very bad 'Class E.'" In addition to rating various sites' terms of service, it also highlights key provisions in those agreements, including whether or not you will be informed if a law enforcement agency has requested information on you or whether your terms of use can be changed at any time, or not, and with or without notice to you. Remember, just because you aren't paranoid doesn't mean that there isn't someone out there watching you.

Endnotes

[1] FTC Complaint; *In the Matter of Designerware, LLC, a limited liability corporation*, FTC File No. 1123151, Federal Trade Commission (the "FTC Complaint").

[2] FTC Complaint, ¶ 5.

[3] FTC Complain, ¶ 6

[4] FTC Agreement Containing Consent Order, p.6.

[5] Mich. Com. Laws § 445.1711-1715.

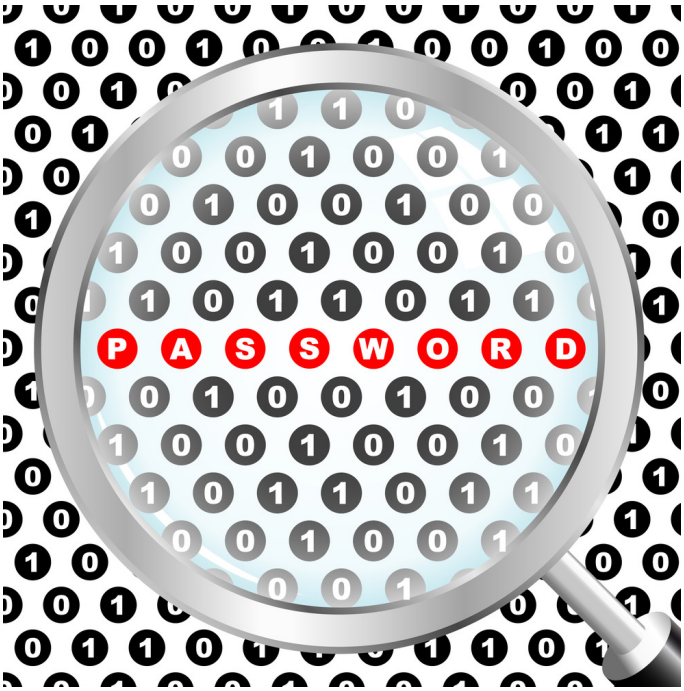
[6] Order Granting Defendant's Motion to Dismiss, *Deacon v. Pandora Media, Inc.*, Case No. C 11-04674 SBA, p.3.

Peter N. Ives is in-house counsel for the Trust for Public Land, where he advises the GIS Division on licensing and contract issues, as well as working on conservation transactions. He also enjoys crafting policy as a city councilor for the City of Santa Fe. He is a graduate of Harvard College and Georgetown University law Center.

Password Protection:

Increasing Security While Maintaining Your Sanity

By Jeffrey H. Albright



Security experts estimate that more than one billion hacking attempts were made worldwide in 2012, and yet people remain largely apathetic about their online passwords.[1] The sobering reality is that most people will eventually get hacked. Nicole Perlroth, who writes on cybersecurity for the *New York Times*, describes her own experience:

> "I set up unique, complex passwords for every Web site, enabled two-step authentication for my e-mail accounts, and even covered up my computer's Web camera with a piece of masking tape—a precaution that invited ridicule from friends and co-workers who suggested it was time to get my head checked.
>
> But recent episodes offered vindication. I removed the webcam tape . . . only to see its light turn green a few days later, suggesting someone was in my computer and watching. More recently, I received a text message from Google with the two-step verification code for my Gmail account. That's the string of numbers Google sends after you correctly enter the password to your Gmail account, and it serves as a second password. The only problem was that I was not trying to get into my Gmail account. I was nowhere near a computer. Apparently somebody else was."[2]

Perlroth's experience is not uncommon. As she points out in her article, everyday hackers are looking for passwords to sell on auction-like market sites "where a single password can fetch $20."[3] Password-cracking programs can also be purchased that can test millions of passwords per second. But there are measures that can be used to increase your own security and to make hacking into your accounts more difficult and less attractive to would-be hackers. Here are measures you can take, gleaned from multiple sources and from my own personal experience, to provide better password protection.

- Do not use the same password for more than one account—ever. Same goes for "challenge questions." If you DO use the same password for an account, use different challenge questions for the second account.
- Make challenge questions more challenging. For example, if you grew up on Dogwood Street, instead of using "Dogwood" or "DogwoodStreet," add the number in front of the name so it becomes "11224 Dogwood Street." Instead of identifying the hometown in which you were born (perhaps readily available to a hacker looking at your Facebook page), list the hospital in which you were born. For example, instead of "Baltimore, MD," list "Eastside Medical Center." Remember, THE COMPUTER DOES NOT CARE! One word of caution, however. Security people looking for fraud will frequently look for patterns. A person that lists "coconut-creampies" for her favorite book, movie, AND place of birth may get rejected by the institution's own internal monitoring systems. But the computer does not care if you list "TaleofTwoCities" as your favorite color or "Thirty Shades of Green" as your favorite restaurant.
- Use strong passwords for ALL of your accounts. Don't use strong ones for financials and weaker ones for non-financials.
- Don't click on the "remember this password"—ever. If you are concerned about remembering the password, write it down somewhere, preferably not on sticky notes on your computer, or download a text file and store it on an encrypted password-protected USB drive. Storing passwords on your desktop is not recommended. If malware infects your computer, they will be lost.
- Go Long. A strong eight-character password is easier to crack than a longer weak one. As an example, use upper and lower case (remember there are 26 letters for each space as opposed to the 10 digits for each space if you only use numbers), and using upper and lower case doubles the possibilities for each space. Mixing in some random characters increases the difficulty. Still, you can make them easy to remember. For example, using the website www.passfault.com to evaluate the complexity of passwords, the phrase: "whyRU-askingmethis?" would take about 86661 *centuries* to crack, with 262 quintillion combinations. That's a lot of zeroes.
- Changing Passwords. Changing passwords every 60-90 days may enhance security—or maybe not. Making password changes frequently tends to defeat some of the other "better practices." Employees don't like it. People will tend to use the same password for multiple accounts, or they will tend to jot them down on sticky notes or some other convenient place in order to access and remember them. While changing passwords frequently is not a *bad* thing to do, it only enhances security if other practices are followed.[4]
- Forget the dictionary. Even numbers inserted within words are easily hacked. To repeat, forget the dictionary. Enough said.
- Use a password manager? Maybe not. Perlroth identifies some programs that will help create strong passwords for you and that will

automatically log you into sites as long as you provide one master password. LastPass, SplashData and AgileBits offer password management software for Windows, Macs, and mobile devices but, and you have likely identified the problem, the software still lies on the computer itself. Perlroth mentions that at a security conference in Amsterdam in 2012, hackers demonstrated how easily the cryptography used by many popular mobile password managers could be cracked.[5]

- Use different browsers. Consider using different browsers for different activities; e.g., one browser for your banking, another for web browsing, perhaps another one for checking email. That decreases the chances of catching a virus for your banking accounts when accidentally stumbling across a tainted/infected celebrity news site. Some recent studies have shown that Chrome was the least susceptible to attacks compared to Firefox and Microsoft Internet Explorer.
- Create stronger user accounts. In addition to a strong password, increasing the complexity of your user identification will increase security. These need not be complex. For example, adding a middle initial or middle name to the user account enhances the complexity. This should not be a substitute for some of the other procedures, but it is easy and need not be mind-numbing.
- Use an alternative email account for password resets. Everyone likely forgets a password from time to time and invariably will require a password reset. Most intruders will expect password information to go to your "public" email account, which is easier to discover than a secondary account created specifically for password resets.
- Limit those who have access to your accounts. Even when registering for online accounts, one can decide not to use your real email account. Services such as "10minutemail.com" allow users to register and confirm an online account which self-destructs 10 minutes later.

Advances are being made to enhance security through the use of biometric sensors, such as keystroke patterns or iris scans. Apple has recently acquired AuthenTec, a maker of biometric sensors. Eventually, biometrics may be integrated into the iPhone and other electronic devices, but those systems are not yet in place. However, by using even a few of the suggestions discussed above, you can increase your online and electronic security.

Endnotes

[1] NBCnews.com, Nightly News/Aired on Nov. 20, 2012, "How to Protect Your Online Passwords."

[2] Nicole Perlroth, *The New York Times*, "How to Devise Passwords That Drive Hackers Away," (November 7, 2012).

[3] Id.

[4] http://socialnewsdaily.com/5238/security-protips-for-protecting-yourself-on-social-media-networks/.

[5] http://www.nytimes.com/2012/11/08/technology/personaltech/how-to-devise-passwords-that-drive-hackers-away/.

Jeffrey H. Albright is a partner and a Martindale Hubbell® AV-rated attorney at the law firm of Lewis and Roca LLP. He was the first chair of the Intellectual Property Section and served as chair again in 2012. His practice includes trademark infringement litigation, copyrights, licensing, e-Discovery, trade secrets, work for hire and registrations at the U.S. Patent and Trademark Office.