IADC

International Association of Defense Counsel

The Joan Fullam Irick Privacy Project

Phase IV

Social Media Surveillance

Warrantless Searches Using GPS Surveillance

Sealing your Settlement Agreement from the Public Eye

New Developments in PRC Privacy Laws

Privacy in the Face of New Forms of Electronic Communication

Biometrics and Privacy in Iraq

Signing Your Privacy Away?

Launching Australia's Privacy Law into the 21st Century

Voyeurism in the Computer Age

The Privacy Implications of Arizona's Immigration Law

Privacy and the MMSEA

Privacy Breach Notification under Canadian Privacy Law

Caution: What You Post Can Hurt You!

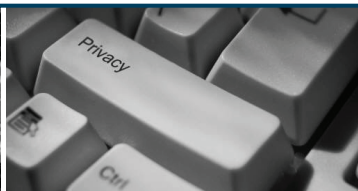
Massachusetts Strengthens Protection Requirements for Consumer Information

Confidentiality Concerns Surrounding Outsourcing

The Judgment of Google

How Companies Should Navigate Foreign Privacy Laws

Revisiting the Apex Doctrine



IADC

International Association of Defense Counsel

The Foundation
of the
International Association of Defense Counsel

303 West Madison, Suite 925
Chicago, IL 60606 USA
p 312.368.1494
f 312.368.1854
e-mail info@iadclaw.org
www.iadclaw.org

The Joan Fullam Irick Privacy Project, Phase IV

Dedication

We dedicate Phase IV of The Privacy Project to the legacy and memory of Joan Fullam Irick, the beloved former President of the IADC.

For those of you who did not have the privilege of knowing Joan and her passion for the IADC Privacy Project, we offer this brief history as so aptly described in the Dedication in Phase II just months after Joan's untimely passing.

This Volume and its earlier companion (published in January 2003) originated from Joan Fullam Irick's deeply held belief that the very concept of privacy faced challenges on many fronts, in the legislature, in the workplace, and in the courts.

Joan's passion for privacy-related issues led her to devote much of her term as President of the IADC to scrutinizing the many ways that our privacy is being invaded. At her urging, The Foundation of the IADC undertook preparations of scholarly papers analyzing the current state of privacy and anticipating future issues in the area.

Throughout the process that produced these volumes, Joan's commitment to the issues imbued all of us with the desire to create a body of high-level, intellectually rigorous white papers that could be used in many disciplines to continue exploration of privacy issues on both the national and international scene, and the foreseeable future of privacy in the individual and corporate worlds.

As 2010-2011 IADC President, Joe Ryan considers Phase IV of The Privacy Project one of his primary initiatives and one that will allow us to share Joan's wonderful legacy with this great organization. In recognition of her commitment to the IADC and the privacy interests of all, we dedicate this undertaking to the memory of Joan Fullam Irick.

Editors

Joseph E. O'Neil, Robert A. Curley, Deborah G. Cole, Tom Finarelli, and Stephen F. McKinney

The Joan Fullam Irick Privacy Project, Phase IV

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual."

- Earl Warren, Chief Justice of the United States Supreme Court, 1963

In 2001, Joan Irick proposed a new project for the Institute of the IADC Foundation. Joan's idea was to create a body of high-level, intellectually rigorous articles exploring national and international privacy issues. The IADC Executive Committee heartily endorsed Joan's proposal to explore this vital area of law. The Foundation Board agreed and The Privacy Project was born, a reflection of Joan's deeply held belief that the very concept of privacy faces ongoing challenges on many fronts, in the legislature, in the workplace, and in the courts. At Joan's urging, a number of authors prepared scholarly papers analyzing the state of privacy and the future of this cherished right.

In January 2003, Phase I of The Privacy Project was published as a dedicated issue of the IADC *Defense Counsel Journal*. It received immediate and positive commentary and critique from many IADC members. With the support of then IADC President Irick, Phase II went to print in January 2004 – several months after Joan's untimely passing. Phase II explored evolving areas of concern in the world of privacy while revisiting and updating earlier issues. Three years later, in 2007, Phase III of The Privacy Project was published to once again address ever emerging and significant privacy issues.

Chief Justice Warren's words are now almost 50 years old, and we can only wonder what he might think today. Phase IV of The Joan Fullam Irick Privacy Project offers a truly global look at emerging and significant privacy issues, from The Peoples Republic of China to Australia, from Italy to Canada and to the United States. This publication explores a wide range of privacy issues including social media, GPS surveillance, biometrics, protection of consumer information, and outsourcing of legal services abroad to name just a few. For the first time, the project includes two articles authored by long-time IADC members and their children who were recently admitted to the practice of law.

The Privacy Project editorial team thanks the authors for their commitment and dedication to this endeavor. The talent and dedication of these individuals form the cornerstone of this publication. The editorial team also wishes to thank Bob Greenlee, Elizabeth Okoro, and Mary Beth Kurzak of the IADC staff, whose efforts made this project possible, and the IADC Foundation for its support.

Table of Contents

IADC
International Association of Defense Counsel

Privacy Project Editors
Joseph E. O'Neil
Robert A. Curley
Deborah G. Cole
Tom Finarelli
Stephen F. McKinney

The Foundation
of the International Association of Defense Counsel

Copyright ©2011 by the International Association of Defense Counsel (IADC) and The Foundation of the International Association of Defense Counsel (Foundation). The Privacy Project is a forum for the publication of topical and scholarly writings on the law, its development and reform, and on the practice of law, particularly from the viewpoint of the practitioner and litigator in the civil defense and insurance fields. The opinions and positions stated in signed material are those of the author and not by the fact of publication necessarily those of the IADC and the Foundation. Material accepted for publication becomes property of the IADC and Foundation, and will be copyrighted as work for hire. Contributing authors are requested and expected to disclose any financial, economic or professional interests or affiliations that may have influenced positions taken or advocated in the efforts.

Social Media Surveillance: Now the Boss Knows What You Did Last Summer…and She Has Some Questions

By Lana Varney and Kimberly King

SOCIAL media may be the antithesis of privacy. After all, it's called "social" media because its users intend for their postings to be viewed by people in their social screen world. While social media arguably diminishes the user's expectation of privacy, some ancient and persistent vestiges of privacy concepts linger over social media postings.

For the workplace, social media has become a window for employers to see inside their employees' personal, and not so personal, lives. Employers who want to track employees' (or potential employees') use of social media, and act on what they see, are challenging whether the traditional legal concepts for protecting privacy should attach to users of social media.

Technology continues to outpace the law that governs it. As a result, case law in the United States is sparse as to the rights and limitations of an employer who seeks to monitor its employees' social media activities. Generally, employers may monitor an employee's social media use and make employment decisions based upon the content of the employee's online website or profile. But employers must be cautious with social media monitoring, especially in two main areas: (1) that the employer obtained the social media information properly and (2) that the employer does not use the obtained information in an unlawfully discriminatory, retaliatory, or other prohibited manner.

Lana Varney is a partner with Fulbright & Jaworski L.L.P. in Austin, Texas. Her practice involves handling complex litigation in both federal and state courts throughout the United States, emphasizing pharmaceuticals and medical device litigation, including defending multi--district federal litigation, class actions, product liability claims, mass tort claims and personal injury matters. Lana frequently lectures on Social Media, Electronic Discovery and Litigation Avoidance Practices.

Kimberly King is an associate with Fulbright & Jaworski L.L.P. in Austin, Texas. Kimberly practices labor and employment law and handles matters at the administrative, trial and appellate level.

I. What is Social Media?

A. Current Tools and Technologies

"Social media" has been defined as "an umbrella term for social interaction using technology (such as the Internet or cell phones) with any combination of words, pictures, video, or audio."[1] In the beginning, the Internet, or Web 1.0, was "read only." Now, Web 2.0 sites are "interactive and visitors can communicate, collaborate, and socialize with the web host and each other. Users

can share pictures, video, music, articles, or other user-generated content."[2]

Social media is appealing to big and small businesses alike. Indeed, credible companies are increasingly turning to social media both to develop a customer base and to build or maintain brand reputation.[3] Many statistics now available allow companies to track social media usage and effectiveness worldwide. Here are some recent examples:

- 11% of all time spent online in the U.S. is spent on social networking sites.[4]
- Up from 13.8% in 2008, over 25% of U.S. Internet page views occurred at one of the top social networking sites in December 2009.[5]
- In the U.S., 234 million people age 13 and older used mobile devices in December 2009 alone.[6]
- Linkedln has over 75 million users.[7] Twitter now has more than 190 million users, processes approximately 65 million Tweets per day, and registers over 330,000 new users per day.[8]
- As of April 2010, an estimated 41.6% of the U.S. population had a Facebook account.[9]
- With a population of over 550 million users, roughly one twelfth of the world's population, Facebook would rank as the world's third largest country, behind only China and India.[10]

Given these statistics, more and more companies are compelled to take notice of the significant impact social media can have on the marketplace.

B. Most Commonly Used Social Media Sites

As social media continues to grow and evolve, the ability to reach more consumers globally continues to increase. Twitter, for example, now reaches Japan, Indonesia, and Mexico, among other markets. This helps companies advertise in multiple languages and reach a broader range of consumers.

One of the ways social media is able to grow and evolve is through its variety. Social media takes on a myriad of forms, including these, which every international company, their CEOs and consumers are using, or are about to use:

1. Blogs (e.g., Blogger, LiveJournal, Open Diary, WordPress, Type Pad, Vox, Xanga): Blogs are regularly updated websites (i.e., the entries are in reverse chronological order with the newest entry at the top) that typically combine text, graphics or video, and links to other sites.[11] Blogs are often informal, taking on the tone of a diary or journal entry. There are blogs of all sorts, ranging from very personal to providing mainstream news updates. Blogs also encourage interactive dialogue with followers by allowing readers to leave comments.[12]
2. Microblogging / Presence applications (e.g., Twitter, Yammer, Jaiku, Plurk, Tumblr,

Posterous): Microblogs are comprised of extremely short written blog posts, similar to text messages. Twitter is an example of a microblog service that lets users broadcast short messages, up to 140 characters long ("Tweets"), using computers or mobile phones.[13]

3. Podcasts (e.g., audio sharing): Podcasts (from a blend of "iPod" and "broadcast") are audio or video files that users can listen to or watch on their computers or portable media devices. Podcasts are usually short and often free, and users can subscribe via their computers or portable media devices to receive new podcasts automatically.[14]
4. Social networks and online communities (e.g., Facebook, MySpace, LinkedIn, Friendster, Sermo, Ning, Orkut, Skyrock, Ozone, Xing, Bebo): Social networks are online communities that allow users to connect and exchange information with clients, colleagues, family and friends who share common interests.[15] In many social networks, users create profiles and then invite people to join as "friends." There are many different types of social networks and online communities, many of which are free. The sites typically range from general use to those targeted for a specific demographic or area of interest.[16]
5. Online video share (e.g., YouTube, Blip.tv, Vimeo, Viddler, sevenload, Zideo): Video sharing allows individuals to upload video clips to an Internet website. The website's video host will then store the video on its server and show the individual different types of codes to allow other users on the site to view or comment on the posted video.[17]
6. Widgets: Allegedly short for "window gadget," a widget is a graphic control on a website that allows the user to interact with it in some way. Widgets can be easily posted on multiple websites, often have the added benefit of hosting "live" content, and typically take the form of on-screen tools (e.g., daily weather updates, clocks, event countdowns, stock market tickers, flight arrival and departure information, etc.).[18]
7. Wikis (e.g., Wikipedia, Medpedia, Wetpaint, PBworks): Wikis, derived from the Hawaiian word for "fast," feature technology that creates access to webpages where users are encouraged to contribute to and modify the existing content.[19] A wiki site can be either open or closed, depending on the preferences of its community of users. An open wiki site allows all site users to make changes and view content, while a closed wiki only allows community members to edit and view content.[20]

C. Current Trends in Corporate Use of Social Media Sites

Just a few years ago, commentators pondered if corporations would adopt and use social media tools. Today, the only question is how much do they use them. According to Fulbright & Jaworski L.L.P.'s 2010 Litigation Trends Survey, approximately one fourth of surveyed companies reported using LinkedIn in pursuit of a business purpose.[21] Others reported use of Twitter and/or Facebook.[22] Another recent survey found that 91% of "Inc. 500" companies are reporting use, both internally and for business purposes, of at least one social media site.[23] Surveyed companies overwhelmingly responded that social media has been successful for their businesses.[24] For example, every social media tool studied enjoys at least an 82% success level with business users.[25] Measuring success was determined as improving their communications approach, building internal knowledge, improving marketing and sales, and guaranteeing long-term sustainability and growth.[26]

In August 2009, a research study found that 81% of senior management, marketing, and human resources executives of companies view social media as a valuable tool to build their company's brand and to enhance relationships with customers.[27] However, the study also found that an equal number, 81%, view social media as a corporate security risk.[28] For that reason many organizations do not allow applications like Facebook, Twitter, Linkedln, etc., to be used by employees via their corporate networks.[29] These technologies, however, are difficult to control and can be easily accessed outside of corporate networks. Consequently, companies and executives face difficult issues regarding how to handle the use of social media, both in and outside of company time.

IV. The Use of Surveillance Software by U.S. Employers

A. Increased Use Due to Increased Awareness of Social Responsibility, Corporate Governance, and Compliance Guidelines

There is a burgeoning "cottage" industry of surveillance software providers. The technology, while originally primitive and limited in availability, has advanced in its sophistication dramatically in the past five years. Moreover, the multiple uses for the collected data have inspired the development of software with more precise findings. This in turn has brought the price-point for such software into the reach of many more companies.

Social media monitoring software is perhaps the fastest growing category of surveillance tools. Many companies embrace the technology to gain, competitive business intelligence and attempt reputation management. Vendors of social media surveillance software represent, for example, that the software can identify online postings to determine such things as where conversations about their products occur most often, or how much their products are being discussed versus those of a competitor. Many of

these monitoring tools are available as Software as a Service (SaaS) over the internet, making it easy for companies to access and deploy them.

Some corporations are now turning their surveillance software to monitoring internal company activity. Companies are seeking employee monitoring software applications designed to prevent employee theft and data leakage, and to eliminate inappropriate online activities. Many software surveillance companies pitch their surveillance software to corporations offering "the ability to monitor the social networking communications of their employees" on all major social networks such as Facebook and Twitter.[30] Customers are told, for example, the software "provides granular and real-time tracking to eliminate significant corporate risks" related to: compliance issues, leakage of sensitive information, HR issues, legal exposure, brand damage and financial impact.[31]

B. Available Tools are More Sophisticated than Last Year's tools and the Innovation of New Tools is Increasing Exponentially

Like everything in the computer world, today's technology will be outdated by the time you finish reading this article. Surveillance software is no exception. Basic and inexpensive techniques have always been available. Automating the process via sophisticated software that is installed at the network level will make monitoring more commonplace, say commentators.[32] Some surveillance software purveyors offer applications "deployed discretely on PCs in an organization" with monitoring managed from a centralized location. The difference is where the employer has "access" to the employees' activities – at the network level or at the end point –and the ability to control their communications, computer applications and online activities (not just the information that flows over the network). Some of the surveillance software purveyors represent they can monitor employees' social media activities even from devices like mobile phones, not necessarily provided by the company to the employee.[33]

C. Basic and Inexpensive Methods

Employers can monitor social media use by employees at little or no cost, except for the personnel and work time necessary to operate the on-line search tools. Here are some examples:

- Google Alerts – a content monitoring service, offered by the search engine company Google, that automatically notifies users when new content from news, web, blogs, video and/or discussion groups matches a set of search terms selected by the user. Alerts can be created for each employee's name.
- Facebook Search – Facebook's own search features allows searches by specific names. Searches can be limited to only publicly posted status updates.

The same application can search Twitter conversations.

- TweetDeck – an Adobe AIR desktop application for Twitter, Facebook, LinkedIn, Google Buzz, Foursquare and MySpace. It allows real-time keyword searches, and users can send and receive tweets and view profiles.
- Yahoo Pipes – a web application from Yahoo! that provides a graphical user interface for building data mashups (combinations of data from more than one Web data source into a single integrated Web application) that aggregates web feeds, web pages, and other services. The application works by enabling users to "pipe" information from different sources and then set up rules for how that content should be modified (by an employee's name, for example).
- Desk Tube – a desktop application that allows users to browse and search YouTube videos, and to access Twitter and Facebook accounts all from the same location.
- Spokeo.com – a search engine and self-described "online USA phone book" that aggregates people-related information from purportedly public sources, including phone directories, social networks, marketing surveys, mailing lists, government censuses, real estate listings, and business websites.

D. Mechanistic Methods

> Many vendors offer corporations the ability to monitor various aspects of their businesses via surveillance software. These companies offer software which can monitor a company's business and competitive intelligence via network and server monitoring, website monitoring, and spy software.[34]

Many vendors also offer corporations the ability to monitor the social networking communications of their employees. Some vendors promise desktop-level visibility into employees' activities, and most currently available software can: capture all keystrokes typed, take screenshots of any computer activity, monitor and read all employee communications such as email and instant message conversations, monitor and block software application use on a scheduled basis, monitor and filter Internet use on and off the company network, monitor PCs that never connect to a network, screen all email attachments for sensitive data, track documents to follow all file use (deletions, renaming, moving, etc.), monitor removable media, destroy data remotely, and locate and recover stolen computers.[35]

V. Legal Considerations for Monitoring Employee's Social Media Activities

A. General Privacy Law Considerations When Monitoring Social Media Use

No United States statutes or regulations specifically govern the monitoring of employees' social media use. The Electronic Communications Privacy Act of 1986 ("ECPA"), which is intended to provide individuals with some privacy protection in their electronic communications, has several exceptions that limit its ability to provide protection in the workplace.[36] Consequently, courts seeking to address electronic monitoring of employees must look to the awkwardly fitting laws that more generally govern privacy rights and employment.

Although U.S. courts have long recognized the right to privacy, the protections afforded by the U.S. Constitution address only government action, and so apply only to governmental employees.[37] Many states, however, have extended certain privacy protections to non-governmental employees through state constitutions and statutes.[38] Moreover, a common law right of privacy is recognized in the majority of the American jurisdictions.[39] In fact, the tort action for invasion of the right of privacy, in one form or another, is currently recognized in thirty-six states.[40] Thus, while a legal analysis of the privacy rights of public and private employees differs, the basic principles are very similar.

In sum, the right of privacy protects against "interference with the interest of the individual in leading, to some reasonable extent, a secluded and private life, free from the prying eyes, ears and publications of others."[41] This broad right can give rise to four, separate claims: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of the other's name or likeness; (3) unreasonable publicity given to the other's private life; or (4) publicity that unreasonably places the other in a false light before the public.[42]

Electronic monitoring could most conceivably give rise to the first of those, a claim of unreasonable intrusion upon seclusion. Such a claim could result in liability if the defendant "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns" and such intrusion would be "highly offensive to a reasonable person."[43] For sure, "there is no liability for the examination of a public record concerning the plaintiff. . . . Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye."[44] In other words, the defendant must have intruded into a *private* place. The same principle appears to apply to one's online activities.

Intrusion into a private place is the focus of the Stored Communications Act ("SCA") which has, perhaps, become the primary federal law used to regulate social media monitoring.[45] The SCA is designed to protect *private*, electronic communications.[46] Specifically, the SCA makes it an offense to "intentionally access[ ] without authorization a facility through which an electronic communication service is provided . . .

and thereby obtain[ ] . . . access to a wire or electronic communication while it is in electronic storage in such system."[47] Exceptions to SCA prohibitions include "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user."[48] But the SCA was written before the advent of the Internet and, as a result, "the existing statutory framework is ill-suited to address modern forms of communication" like social media.[49]

Applying the applicable laws, a critical issue is whether an employee has a reasonable expectation of privacy, and that is determined on a case-by-case basis. When evaluating a particular case, some primary considerations may include: whether the employee's social media profile or website is public or private in nature, the employer's social media policy, and the terms and conditions of the social medium itself.

B. Privacy Expectations Will to Some Extent Depend on the Whether the Employee's Profile or Website is Public or Private

When an individual maintains a social media website that is accessible to the general public, he or she cannot have a reasonable expectation of privacy with respect to the content of that site. In *Moreno v. Hanford Sentinel, Inc.*,[50] a California district court rejected an invasion of privacy claim based on information posted on a MySpace page. The named plaintiff, Cynthia Moreno, had posted her opinion about her hometown in an "Ode to Coalinga." The ode began by saying "the older I get, the more I realize how much I despise Coalinga," and then made several negative comments about the town and its inhabitants. Someone forwarded the ode to the editor of the local newspaper who, in turn, published it in the newspaper's letters section. The community reacted violently to the ode, including death threats and a shot at the home of Moreno's family. As a result, Moreno and her family filed suit against the newspaper, claiming public disclosure of private facts.

Affirming the district court's decision, the court of appeals held that the plaintiffs could not state a cause of action for invasion of privacy because the ode was not private.[51]The court found Moreno's publication of the ode on MySpace was an "affirmative act that made her article available to any person with a computer" and "no reasonable person would have had an expectation of privacy regarding the published material."[52] *Moreno* thus shows that a person who openly shares information on a public social media site will likely have little ground to complain when the information is re-published.

In contrast, when an employee maintains a private social media website, he or she will likely receive some protection. To that end, when an online website or profile is truly private, an employer who uses improper means to gain access to such information may be held liable.

A New Jersey jury, for example, awarded two plaintiffs lost wages and punitive damages against an employer found to have accessed a MySpace chat group without authorization.[53] The plaintiffs, employees of a restaurant, had

set up an invitation-only MySpace chat group. In the initial posting, one of the plaintiffs stated that the purpose of the group would be to "vent about any BS we deal with [at work] without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation."[54] After being shown the website by another employee, a manager requested the employee's password to log onto the site. Based on the content viewed, the manager fired the employees who created the site. They responded by bringing an action against the employer, asserting claims of wrongful termination, invasion of privacy, and violations of wiretapping statutes.

Following the verdict, the court denied the employer's motion for judgment as a matter of law and motion for a new tria1.[55] The employer argued that there was no evidence an invited member of the chat group did not authorize the manager to use her password. The court rejected the argument, ruling the jury could reasonably have inferred that the employee's purported authorization was "coerced or provided under pressure."[56] Such coercion would make her consent not voluntary.

Similarly, in *Konop v. Hawaiian Airlines, Inc.*,[57] an airline pilot, who created and maintained a website where he posted bulletins criticizing his employer, was able to survive a motion for summary judgment. Alleging that Hawaiian Airlines, Inc. had viewed his website without authorization, the pilot asserted state tort claims, as well as violations of the federal Wiretap Act, the Stored Communications Act, and the Railway Labor Act. The court found the pilot's website to be private.[58] The pilot controlled access to his website by requiring visitors to log in with a user name and password. He created a list of fellow employees who were eligible to access the website. And he programmed the website to allow access only when a person clicked the "SUBMIT" button on the screen, indicating acceptance of the terms and conditions that prohibited any member of management from viewing the website and prohibited users from disclosing the website's contents.[59]

Despite the pilot's precautions, a Hawaiian Airlines vice president was able to view the website. He did so by obtaining permission from two employees to use their names to gain access to the site. One or both of the employees had never logged onto the website to create an account.

The court of appeals' analysis of the pilot's SCA claim is significant. Hawaiian argued that it was exempt from liability under the SCA because Section 2701(c)(2) of the act allows a person to authorize a third party's access to an electronic communication if the person is (1) a "user" of the "service" and (2) the communication is "of or intended for that user."[60] The district court granted summary judgment for Hawaiian, but the court of appeals reversed, finding that the plain language of Section 2701(c)(2) indicates that only a "user" of the service can authorize a third party's access to the communication.[61] The statute defines "user" as one who (1) uses the electronic communications service and (2) is duly authorized by the provider of such service to engage in such use.[62] Finding no evidence that the consenting employees actually used the website, as opposed to

merely being eligible to use it, the court held that the Section 2701(c)(2) exception did not apply.[63] This decision shows not only that a court may recognize one's privacy when the person takes great steps to protect it, but also that employers cannot use unauthorized means to monitor their employees.

C. Privacy Expectations May Depend on an Employer's Policies and Practices.

The employer's written policies and practices may also become important in determining an employee's privacy rights. Courts are focusing on any evidence that employers affirmatively took steps to inform employees of policies or regulations that govern their social media use. Although courts are just starting to grapple with the impact of employer policies on social media use, courts firmly embrace using employer policies to determine the privacy expectations for employee emails.[64] To measure privacy expectations for employee emails, the court in *In re Asia Global* formed, and other courts have adopted, the following test: (1) is there a corporate policy; (2) does the company monitor employee email use; (3) do third parties have a right of access; and (4) did the company notify the employee or did the employee know about the use and monitoring policies?[65]

While it can be anticipated courts reviewing privacy expectations related to social media will make similar analyses, the full value of any guidance by the above factors is uncertain. A potentially persuasive argument can be made that social media is simply the next generation of electronic mail, and that courts should extend their analysis of employee privacy expectations for emails to employee privacy expectations for social media. Conversely, the argument can be made that there are inherent differences between social media and email, and that those differences substantially diminish any privacy expectations for social media. It can be argued, for example, that social media (unlike email) is specifically designed to reach a large number of people. Posting information on a social media site is not just like sending an email. It is like sending a mass email.

In addition, it appears only two states—Delaware and Connecticut—require employers who engage in electronic monitoring to give written notice to their employees.[66] The Connecticut statute sets forth noteworthy exceptions; it allows an employer to monitor without prior notice when "an employer has reasonable grounds to believe that employees are engaged in conduct which (i) violates the law, (ii) violates the legal rights of the employer or the employer's employees, or (iii) creates a hostile workplace environment, and (B) electronic monitoring may produce evidence of this misconduct."[67] Employers in the remaining 48 states can argue that the absence of a statutory duty to provide notice of electronic monitoring suggests an absence of privacy rights.

In any event, the analyses for determining an employee's privacy rights will likely be fact specific, thus an employer's policy and practice regarding social media will likely be analyzed to evaluate whether an employee's expectation to privacy is reasonable.

Consequently, prudent companies have come to adopt written social media

polices to regulate their employees' social media activity.[68] The following points, where appropriate, should be considered for inclusion in social media policies:

- A clear statement that misuse of social media can be grounds for discipline, up to and including termination;
- A prohibition on disclosure of the employer's confidential, trade secret or proprietary information;
- A request that employees keep company logos or trademarks off their blogs and profiles and not mention the company in commentary;
- An instruction that employees not blog or post during business hours, unless for business purposes;
- A request that employees bring work-related complaints to human resources before blogging or posting about such complaints;
- A prohibition on using company e-mail addresses to register for social media sites;
- A prohibition on posting false information about the company or its employees;
- A general instruction that employees use good judgment and take personal and professional responsibility for what they publish online;
- A demand that all employees with personal blogs that identify the employer include a disclaimer that the views expressed on the blog are those of the individual and not the employer;[69] and
- A prohibition on "Friending" members of management by non-management personnel, and vice versa.

D. Privacy Expectations May Depend on the Terms and Conditions of the Social Medium.

Social media sites do not "guarantee complete privacy," so a court may conclude that the employee or applicant cannot have a reasonable expectation of privacy.[70] In fact, Facebook's privacy policy expressly states:

> Risks inherent in sharing information. Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook . . . .[71]

A New York Supreme Court recently relied upon the terms and conditions of Facebook and MySpace to reject a personal injury plaintiff's objection to production of material on those sites.[72] The defendant moved for an order

granting it access to the plaintiff's current and historical Facebook and MySpace pages on the grounds that the plaintiff had placed information on the sites that was inconsistent with her claims concerning the extent and nature of her injuries, especially her claims for loss of enjoyment of life.[73]

Ordering the plaintiff to grant the defendant access to her Facebook and MySpace pages, the court relied, in part, upon the policies of those sites. The court noted that Facebook policy states "`Facebook is about sharing information with others" and that MySpace "is self-described as an `online community' and as a 'global lifestyle portal that reaches millions of people around the world.'"[74] As the court also pointed out, "MySpace warns users not to forget that their profiles and MySpace forums are public spaces and Facebook's privacy policy set[s] forth, *inter alia*, that: 'You post User Content . . . on the Site at your own risk . . . .'"[75] Because neither Facebook nor MySpace guarantees "complete privacy," and because the plaintiff when creating her accounts consented to the sharing of her personal information, the court held that the plaintiff had no legitimate reasonable expectation to privacy. Finally, the court concluded that "given the millions of users, . . . privacy is no longer grounded in reasonable expectations, but rather in . . . wishful thinking.'"[76]

VI. Adverse Employment Actions Based on Social Media Activities

As a general rule, an employer is allowed to consider information on an applicant's or current employee's social media profile or website when making employment decisions. This general rule, however, is rife with limitations based in general employment laws.

A. Hiring

Employers certainly use social media sites to vet job candidates. Perhaps the most notable example of such vetting occurred in March 2009 when an applicant offered a job by Cisco tweeted, "Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work."[77] Soon thereafter, a Cisco employee posted this reply: "Who is the hiring manager. I'm sure they would love to know that you will hate the work. We here at Cisco are versed in the web."[78]

But use of social media information during the hiring process may create liability risks for employers. For instance, an employer is still obligated to adhere to civil rights laws. Title VII of the Civil Rights Act of 1964 (Title VII), as amended, prohibits employment discrimination based on race, color, religion, gender and national origin.[79] In addition, the Americans with Disabilities Act of 1990, as amended, prohibits discrimination on the basis of disability.[80] Social media profiles often reflect personal attributes that qualify a person as part of a protected group under these statutes. A profile may reveal an applicant's gender, race, national origin, religious beliefs, age, health problems, political affiliations, sexual orientation and even whether the person plans to have children. Because an adverse employment action based on a person's

protected status is strictly prohibited whatever the source of the information, an employer monitoring social media should target only information relevant to the applicant's abilities and qualifications for the particular job position.

In addition to civil rights laws, social media inquiries may be subject to limitations by the Fair Credit Reporting Act ("FCRA").[81] The FCRA is designed to protect the privacy of consumers' credit report information and to guarantee that the information supplied by credit reporting agencies is as accurate as possible.[82] Sections 604, 606, and 615 of the FCRA help ensure that applicants or current employees are not denied employment opportunities due to inaccurate or incomplete consumer credit reports. Those sections thus set forth certain responsibilities of employers when using consumer credit reports to hire new employees or evaluate current employees for promotion, reassignment, or retention.

Under the FCRA, if an employer uses a third party service to conduct certain types of background checks, the employer must give prior notice of the check to the individual being investigated. Some states have enacted more restrictive "FCRA plus" laws, which require prior notice and consent from the applicant even if the employer does not use a third party to do the search.[83] Because prior notice affords an applicant time to remove offensive material before the search begins, it potentially defeats the purpose of a social media inquiry.

It is still unclear whether social media profiles are covered under the FCRA. The FCRA provides the following definitions:

- "The term 'consumer report' means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, *character*, *general reputation*, *personal characteristics*, *or mode of living* which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for . . .employment purposes;"[84] and
- "The term 'investigative consumer report' means a consumer report or portion thereof in which information on a consumer's *character, general reputation, personal characteristics, or mode of living* is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information."[85]

So while the legislature and courts have not definitively found that social media monitoring triggers FCRA protections, the above definitions certainly appear broad enough to include reports of a consumer's social media use.

B. Discipline and Discharge

As with hiring, many employers have disciplined or even discharged employees for inappropriate messages on social media.[86] Just recently, a math and science teacher was asked to resign after she complained on Facebook about her job, describing students as "germ bags" and school parents as "snobby" and "arrogant."[87] Notably, the teacher claimed that she had arranged her privacy settings to limit her profile to selected friends, but Facebook later defaulted her settings to allow viewing by the wider Facebook community.[88]

While many employers have similarly disciplined or discharged employees for comments or other postings on social media sites, such employment actions could run afoul of employment laws. For sure, the same civil rights laws and FCRA considerations described above regarding the hiring process also apply to current employees.

In addition to those considerations, several states prohibit employers from taking adverse action against a current employee for engaging in lawful, conduct while the employee is not at work. Such statutes vary in scope. On one end of the spectrum, several states protect a single, specific activity—such as lawful tobacco use.[89] On the other end, a few states—such as California, New York, and Colorado—protect all "lawful conduct occurring during nonworking hours away from the employer's premises."[90] In particular, New York restricts employers from taking *any* adverse employment action against employees engaged in "recreational activities," meaning "any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for recreational purposes, including but not limited to sports, games, hobbies, exercise, reading and the viewing of television, movies and similar material."[91] Exceptions to these statutes may apply, such as when the employer's restrictions are related to a bona fide occupational qualification, or are necessary to avoid a conflict of interest with the employees' responsibilities.[92]

These "off-duty activity" statutes may be implicated by social media in numerous ways. For example, the statutes may certainly limit an employer's ability to terminate an employee who posts photographs of himself smoking tobacco. The broader statutes generally protecting "lawful conduct" or "recreational activities" could also limit an employer's ability to hire, terminate, or make other employment decisions based on information gleaned from an employee's social media page. Indeed, in states embracing broad off-duty activity statutes, one could argue that participating in social media sites, such as posting photographs on Facebook, blogging, or even "tweeting" rants about a supervisor, is a "recreational activity" itself and that adverse employment actions based on such participation is unlawfully discriminatory. But, if such participation creates a conflict of interest with the employees' responsibilities (e.g., negatively impacts an employer's business interest, customer relations, product image, or coworkers' rights), an adverse action may be justified.

Also, the National Labor Relations Act ("NLRA") makes it an unfair labor

practice "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in [Section 7 of the NLRA]."[93] Section 7 sets forth several rights, including the right "to engage in . . . concerted activities for the purpose of collective bargaining or other mutual aid or protection."[94] The National Labor Relations Board ("NLRB") has held that an employer's actions violate Section 7 if those actions would "reasonably tend to chill employees" in the exercise of their rights under the NLRA.[95]

Recently, the NLRB announced its plans to prosecute a complaint under Section 7 against American Medical Response of Connecticut, regarding the termination of an employee who posted negative remarks about her supervisor on her Facebook page.[96] The matter began when an employee was asked to prepare a report related to a customer's complaint about the employee's work. The employee asked for union representation regarding the complaint, and the company denied her request. The employee then posted a negative comment about her supervisor on her Facebook page, which elicited responses from coworkers and led to further negative comments by the employee. As a result, the company fired the employee, citing violations of the company's internet policies, which prohibited employees from making disparaging remarks about their employer or supervisors. The NLRB determined that the Facebook postings constituted "protected concerted activity" under Section 7 of the NLRA and that the company's internet policy was overly broad. While the outcome of this matter is pending, previous guidance has made clear that employees do not have unlimited discretion to publicly criticize their employers under the protections of the NLRA.

For example, in *Endicott Interconnect Technologies, Inc. v. NLRB*, the court found that an employee's online communications were not protected under Section 7 as they were disloyal to his employer.[97] As background, after Endicott Interconnect Technologies ("EIT") permanently laid off 200 employees, an employee (who kept his job) was cited in a newspaper article, commenting on his disagreement with the layoff.[98] In response, an EIT owner reprimanded the employee for his comments. Thereafter, the employee posted on a public website a message that included: "This business is being tanked by a group of people that have no good ability to manage it. They will put it into the dirt just like the companies of the past. . . ."[99] As a result, EIT discharged the employee.[100]

The *Endicott* court found that the employee's communications were not protected by Section 7 of the NLRA. The court explained that an employee's communication to a third party is deemed protected under Section 7 only if: (1) "it is related to an ongoing labor dispute" and (2) "it is 'not so disloyal, reckless or maliciously untrue as to lose the Act's protection.'"[101] The court found the employees' communications were "unquestionably detrimentally disloyal."[102] Thus, the court concluded that EIT did not violate the Act when it discharged the employee.

Similarly, in Sears Holdings, the NLRB's Office of General Counsel issued an opinion memorandum concluding an employer's social media

policy did not violate Section 8(a)(1).[103] The employer had issued a social-media policy regarding its employees' use of blogs, social networks, and other social media. The policy listed several subjects that employees were not permitted to discuss online. The union filed an unfair-labor-practice charge, alleging that the policy violated the NLRA.

In short, the Office of General Counsel concluded that the employer's policy did not violate the NLRA because it could not reasonably be interpreted in a way that would chill activity under Section 7 of the NLRA.[104] The memorandum explained that a review of a complained-of social media policy requires an evaluation of the policy as a whole, as "a rule's context provides the key to 'reasonableness' of a particular construction."[105] The general counsel concluded that Sears' policy against "[d]isparagement of company's . . . executive leadership, employees, [or] strategy . . . "provided sufficient context to preclude a reasonable employee from construing the rule as a limit on Section 7 conduct."[106]

Given the decisions in *Endicott* and *Sears Holdings*, an employee cannot use Section 7 of the NLRA as a complete shield from discipline or discharge. These decisions also highlight the value of a clear social media policy.

C. Unintended Consequences of Social Media Monitoring

An employer who chooses to monitor its employees' social media activity may be subject to some unintended consequences. While these consequences are beyond the scope of this article, employers should be mindful of them. In short, social media monitoring can provide an employer too much information. A few issues social media monitoring may raise include: employee records retention; unlawful collection of health records; discrimination and retaliation claims based on the failure to apply employment policies fairly; and expensive litigation discovery.

One of the main drawbacks to social media monitoring is that an employer may become more susceptible to claims where liability is based on the employer's knowledge of an employee's inappropriate conduct. For example, if an employee posts a discriminatory remark about a co-worker on the employee's Facebook page, an employer monitoring that page may be unable to successfully claim lack of knowledge of the posting.[107] Similarly, an employer can be held vicariously liable for its employee's defamatory statements. Again, if an employer acquires knowledge of the defamatory remark (by way of monitoring or otherwise), it may be easier to impose liability on the employer.[108] To be clear, employers have no affirmative duty to scrupulously police employees' social media activities. If, however, the employer in fact becomes aware of inappropriate social media activity that impacts the workplace, the employer must take appropriate action. Otherwise, the employer may be perceived as condoning the inappropriate activity.

VII. Conclusion

As employee use of social media continues to increase, employers have a lot of windows through which to see their

employees. The technical ability to monitor social media is rapidly improving. Not only are monitoring tools more sophisticated and accurate now than they were a year ago, the innovation of new tools continues to increase exponentially.

Employers must, however, take care to avoid the legal pitfalls in monitoring employee social media activities. Thus, employers should consider all the circumstances of its social media monitoring, including whether the means of obtaining information are proper and authorized, whether the information is public or private in nature, the type of information they choose to monitor and whether the information is related to a protected status under civil rights laws, and how the employee uses such information to make employment decisions.

---

[1] Debra L. Bruce, "*Social Media 101 for Lawyers,"* TEX. BAR J., Vol. 73, No. 3 186 (2010)

[2] *Id*.; *see also* Alan J. Bojorquez & Damien Shores, *Article: Open Government and the Net: Bringing Social Media Into the Light*, 11 TEX. TECH. ADMIN. L.J. 45, 47 (2009) (explaining that social media is "'the democratization of information, transforming people from content readers into content publishers.'") (citation omitted).

[3] *See* Anthony L. Hall & Deanna C. Brinkerhoff, "Implementing an effective social media policy," NEVADA EMPLOYMENT LAW LETTER Vol. 15, Issue 6, Mar. 2010 (noting that social media is "becoming an increasingly common method of communication for companies and their employees").

[4] Lee Ann Prescott, "54% of US Internet users on Facebook, 27% on MySpace," VENTUREBEAT, Feb. 10, 2010, http://digital.venturebeat.com/2010/02/10/54-of-us-internet-users-on-facebook-27-on-myspace/ (last visited Apr. 12, 2010).

[5] *Id.*

[6] *Id.*

[7] About Us: Latest Linkedln Facts, Linkedln.com, http://press.linkedin.com/about (last visited Dec. 15, 2010).

[8] "A Conversation with Dick Costolo, COO, Twitter," CM Summit, June 7-8, 2010, *available at* http://cmsummit.com/Gallery.

[9] Roy Wells, *41.6% of the US Population Has a Facebook Account*, Social Media Today, http://socialmediatoday.com/roywells1/158020/416-us-population-has-facebook-account (last visited Jan. 15, 2011).

[10] Lev Grossman, *Person of the Year 2010: Mark Zuckerberg*, TIME, Dec. 15, 2010, *available at* http://www.time.com/time/specials/packages/article/0,28804,2036683_2037183_2037185,00.html. Interestingly, Facebook is banned in China. April Rabkin, *The Facebooks of China*, FAST COMPANY, Jan. 12, 2011, available at http://www.fastcompany.com/magazine/152/the-socialist-networks.html.

[11] HHS Center for New Media, "Social Media 101 Overview: The WHAT and the WHY," *available at* http://newmedia.hhs.gov/SocialMedia101Overview06-29-09.pdf.

[12] *Id.*

[13] "Micro-Blogs," Social Media Training, http://socialtraining.Wetpaint.com/page/Micro-Blogs (last visited Jan 5, 2011).

[14] HHS Center for New Media, *supra* note 11.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] Wikis, ""Webcontent.gov, http://www.usa.gov/webcontent/technology/wikis.shtml (last visited Apr. 12, 2010).

[21] FULBRIGHT & JAWORSKI L.L.P., FULBRIGHT'S 7TH ANNUAL LITIGATION TRENDS SURVEY REPORT 55 (2010), *available at* http://www.fulbright

.com/index.cfm?fuseaction=publications.PremiumDownloadDetailNew&pub_id=4665&site_id =391&detail=yes.

[22] *Id.*

[23] Tamara Schweitzer, "Study: Inc. 500 CEOs Aggressively Use Social Media for Business," INC., Nov. 25, 2009, http://www.inc.com /news/articles/2009/11/inc500-social-media-usage.html# (last visited Apr. 12, 2010), citing Nora Ganim Barnes, Ph.D. & Eric Mattson, Center for Marketing Research, "Social Media in the 2009 Inc. 500: New Tools & New Trends," 2009, *available at* http://www.umassd.edu/cmr/studiesresearch/socialmedia2009.pdf.

[24] Nora Ganim Barnes, Ph.D. & Eric Mattson, Center for Marketing Research, "Social Media in the 2009 Inc. 500: New Tools & New Trends," 2009, *available at* http://www.umassd.edu/cmr/studiesresearch/socialmedia2009.pdf.

[25] *Id.*

[26] "Social Media Research and Trends: Do Top Brands Adopt and Use Social Media Tools?" http://webcache.googleusecontent.com/search?q=cache:ruq3p-1Ku_oJ:www.mastemewmedia.org/social-media-research-and-trends-do-top-brands-adopt-and-use-social-mediai+Measuring+success+was+determined+as+improving+their+communications+approach,+building+intemal+knowledge,+improving+marketing+and+sales+as+well+as+guaranteeing+longterm+sustainability+and+grovvth.&cd=l&h1=en&ct=clnk&gl=us (last visited Apr. 13, 2010).

[27] *See* Russell Herder & Ethos Business Law, "Social Media: Embracing the Opportunities, Averting the Risks," Aug. 2009, *available at* http://www.russell herder.com/SocialMediaResearch/.

[28] *Id.*

[29] FULBRIGHT & JAWORSKI L.L.P., FULBRIGHT'S 6TH ANNUAL LITIGATION TRENDS SURVEY REPORT (2009), *available at* http://www.fulbright.com/litigationtrends06

[30] *E.g.*, Teneros Social Sentry, http://www.teneros.com/socialsentry/ (last visited Jan. 5, 2011).

[31] *Id.*

[32] *See e.g.*, Joshua Brustein, *Keeping a Closer Eye on Employees' Social Networking*, N.Y. TIMES (Mar. 26, 2010).

[33] *See id.*

[34] *See* http://www.activitymonitoringsoftware.com/ (last visited Jan. 15, 2011) (listing common vendors including but not limited to: Spiceworks, FuseStats, WebCam Corp., Advanced Spy, CompetitiveVision, Capturix, Compete, F1exiSPY, Logaholic, SAP Business Objects, and PhoneStealth).

[35] *See*, *e.g.*, http://www.interguardsoftsoftware.com/websense.asp (last visited Jan. 15, 2011).

[36] For example, the act does not prevent access to electronic communications by system providers, which could include employers who provide the necessary electronic equipment or network to their employees. *See, e.g.,* U.S. v. McLaren, 957 F. Supp. 215 (M.D. Fla. 1997).

[37] *See e.g.,* City of Ontario, Cal. v. Quon, 130 S.Ct. 2619, 2627-28 (2010) ("The Fourth Amendment applies as well when the Government acts in its capacity as an employer.") (internal citation omitted); 15 Causes of Action 2d 139 §§ 1-2 (Sept. 2010) ("A § 1983 claim may also lie for violation of the public employee's implied constitutional rights to privacy which have been interpreted by the United States Supreme Court as falling within the 'penumbra' of several constitutional amendments (and as applied to the states through the Fourteenth Amendment). A Section 1983 claim for violation of the employee's constitutional rights to privacy will not lie as against a private employer.")

[38] *E.g.,* CAL. CONST., ART. I, §1; ARIZ. CONST. ART. II, §8, MONT. CONST. ART. II, §10, WASH. CONST. ART. I, §7.

[39] 82 Am. Jur. 2d Wrongful Discharge § 165 (July 2010); Restatement (Second) of Torts § 652A, cmt. a (1977).

[40] Restatement (Second) of Torts § 652A, reporter's n. (1977) (identifying a right to privacy in following states: Alabama, Alaska, Arizona, Arkansas, California, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Mexico, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, and West Virginia).

[41] *Id.* at cmt. b.

[42] Restatement (Second) of Torts § 652A.

[43] Restatement (Second) of Torts § 652B.

[44] *Id.* at cmt. c.

[45] 18 U.S.C. §§ 2701-2711 (2000). In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848, to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, 18 U.S.C. §§ 2510-2522 (2000), which previously addressed only wire and oral communications, to also include electronic communications. S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. Title II of the ECPA created the Stored Communications Act ("SCA"), which was designed to "address[ ] access to stored wire and electronic communications and transactional records." *Id*.

[46] *See* S. Rep. No. 99-541, at 35-36, 1986 U.S.C.C.A.N. at 3599 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to ... electronic or wire communications that are not intended to be available to the public.").

[47] 18 U.S.C. § 2701(a)(1).

[48] 18 U.S.C. § 2701(c)(2).

[49] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir 2002), *cert. denied* 537 U.S. 1193 (2003) (mem).

[50] 91 Cal. Rptr.3d 858 (Cal. Ct. App. 2009).

[51] *Id.* at 862-63.

[52] *Id.*

[53] *See* Pietrylo v. Hillstone Rest. Group., No. 06-5754, 2009 WL 3128420, *1 (D.N.J. Sept. 25, 2009) (not for publication).

[54] Pietrylo v. Hillstone Rest. Group., No. 06-5754, Order and Opinion denying Defendant's Motion for Reconsideration of this Court's July 24, 2008 Opinion and Order, which granted in part and denied in part Defendant's Motion for Summary Judgment (Feb. 25, 2008) (Doc. 31) (not for publication).

[55] *Pietiylo*, 2009 WL 3128420, at * 6.

[56] *Id.* at *3.

[57] 302 F.3d 868 (9th Cir. 2001).

[58] *Id*. at 875, 876, n. 3.

[59] *Id*. at 876, n. 3.

[60] 18 U.S.C. § 2701(c)(2); *See also Konop*, 302 F.3d at 879.

[61] *Konop*, 302 F.3d at 880.

[62] 18 U.S.C. § 2510(13).

[63] *Konop*, 302 F.3d at 880.

[64] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005); Brown-Criscuolo v. Wolfe, 601 F. Supp.2d 441, 449 (D. Conn. 2009); Gates v. Wheeler, No. A09-2355, 2010 WL 4721331, *6 (Minn. App. Nov. 23, 2010).

[65] *In re Asia Global Crossing, Ltd*., 322 B.R. at 257; *see also Brown-Criscuolo*, 601 F. Supp.2d at 449; Gates, 2010 WL 4721331, *6.

[66] See CONN. GEN. STAT. ANN. § 31-48D(B)(1) (2011); DEL. CODE. ANN. TIT. 19, § 705 (2011).

[67] CONN. GEN. STAT. ANN. § 31-48D(B)(1) (2011).

[68] *See* Matt Leonard, *Lawsuits and PR Nightmares: Why You Need a Social Media Policy*, SOCIAL ENGINE J., Aug. 18, 2009 http://www.searchenginejournal.com/why-employees-need-social-media-guidelines/12588// (listing, among others, social media policies of Dell, Intel, IBM, Wells Fargo, Greteman Group, and Cisco); see also http://walmartstores.com/9179.aspx and http://www.ibm.com/blogs/zz/en/guidelines.html.

[69] Renee M. Jackson, Social *Media Permeate the Employment Life Cycle*, NAT'L L. J. (Jan. 11, 2010).
[70] *C.f.* Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. 2010) (holding personal injury plaintiff had no reasonable expectation of privacy for information shared through social media).
[71] Facebook's Privacy Policy, Facebook.com, http://www.facebook.com/policy.php (last revised Dec. 22, 2010).
[72] *Romano*, 907 N.Y.S.2d at 656-54.
[73] *Id.* at 651.
[74] *Id*. at 653-54 & nn. 1-3 (*quoting* Facebook Principles, http://www.facebook.com/policy.piph (last visited April 3, 2009); About Us, Myspace.com/index.dfm?fuseaction=misc.aboutus (last visited June 16, 2009); MySpace Safety Highlights, http://www.myspace.com/index.cfm?frseaction=cms.veiwpageplacement=saftety (last visited June 18, 2009).
[75] *Id*. at 656 & nn. 7-8 (quoting MySpace General Tips, http://www.myspace.com/index.cfm?frseaction=cms.veiwpage&placement=safety-pagetips (last visited June 18, 2009; Facebook Principles-Effective as November 26, 2008, http:www.facebook.com/policy.php (last visited June 18, 2009).
[76] *Id*. at 657& n. 9 (quoting Dana L. Flemming and Joseph M. Herlihy, *Department*: *Heads Up*: *What Happens When the College Rumor Mill Goes OnLine? Privacy, Defamation and Online Social Networking Sites*, 53 B.B.J. 16 (Jan./Feb. 2009)).
[77] Samantha Rose Hunt, *How to use technology wrong*, TG DAILY (Mar. 18, 2009), http://www.tgdaily.com/trendwatch-opinion/41777-how-to-use-technology-wrong.
[78] *Id.*
[79] 42 U.S.C. §§ 2000e-2000e-17 (2008).
[80] 42 U.S.C. §§ 12101-12181 (2010).
[81] 15 U.S.C. §§ 1681-1681(v) (2000).
[82] 15 U.S.C. §§ 1681 ("There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."
[83] *E.g.*, CAL. CIV. CODE § 1785.20.5.
[84] 15 U.S.C. § 1681a(d) (Emphasis added).
[85] 15 U.S.C. § 1681a(e) (Emphasis added).
[86] *See* Catharine Smith & Bianca Bosker, *Fired Over Twitter: 13 Tweets That Got People CANNED*, HUFFINGTON POST (Sept. 14, 2010), *http://www.huffingtonpost.com/2010/07/15/fired-over-twittertweetsn_645884.html#s112801*.
[87] *Facebook Faux Pas Leads to Teacher Losing Job*, CBSNews.com (Aug. 20, 2010) *available at* http://www.cbsnews.com/stories/2010/08/20/earlyshow/main6789897.shtml (last visited Jan. 15, 2011).
[88] *Id.*
[89] *E.g.*, ARIZ. REV. STAT. ANN. § 36-601.01(f) (2011); CONN. GEN. STAT. ANN. § 31-40S (West 2011); LA REV. STAT. ANN. § 23:966 (2011); MO. ANN. REV. STAT. § 290.145 (West 2011); NJ STAT. ANN. § 34:6B-1 (West 2011); TENN. CODE ANN. § 50-1-304 (West 2011).
[90] *E.g.*, CAL. LAB. CODE §§ 96(k), 98.6 (West 2011); *Accord* N.Y. LAB. LAW § 201-d (McKinney 2011); COLO. REV. STAT. §24-34-402.5 (2007).
[91] N.Y. LAB LAW § 201-d (McKinney 2011). Colorado's statute is slightly narrower than New York's and California's statutes; it only protects employees from termination. Colo. Rev. Stat. §24-34-402.5 (2007).
[92] *See* N.Y. LAB. LAW § 201-d (McKinney 2011).
[93] 29 U.S.C. § 158(a)(1).
[94] 29 U.S.C. § 157.
[95] *Martin Luther Mem. Home, Inc*, 326 NLRB 826 (1998).
[96] Steven Greenhouse, *Company Accused of Firing Over Facebook Post*, N.Y. TIMES, (November 8, 2010) http://www.nytimes.com/2010/11/09/business/09facebook.html?_r=3&adxnn1=1&adxnnlx=1289358911-EgmLbp7Ie0cXnExZ5bY4yw.
[97] 453 F.3d. 532, 537-38 (D.C. Cir. 2006).
[98] *Id*. at 533-34.
[99] *Id*. at 534-35.

[100] *Id.* at 535.
[101] *Id*. at 536-37 (citing NLRB v. Electrical Workers Local 1229, 346 U.S. 464 (1953) (other citations omitted).
[102] *Id*. at 537.
[103] Op. Gen. Counsel, N.L.R.B., No.18-CA-19801, 2009 WL 5593880, *1 (Dec. 4, 2009).
[104] *Id.*
[105] *Id.* at *3.
[106] *Id*. at *3-4.
[107] *See* Blakey v. Cont'l Airlines, Inc., 751 A.2d 538, 542-43 (N.J. 2000) (The plaintiff sued her employer, alleging workplace discrimination in violation of Title VII of the 1964 Civil Rights Act, 42 U.S.C.A. § 2000e *et seq.* Several male employees, in response to the lawsuit, published messages about the plaintiff on an on-line electronic bulletin board used by employees. The plaintiff considered the messages as harassing, false and defamatory. The court held that the electronic bulletin board could be so closely related to workplace environment and beneficial to the employer that continuation of harassment on the bulletin board should be regarded as part of the workplace. The court also held that if the employer had notice that the co-employees were engaged in a pattern of retaliatory harassment towards plaintiff, the employer would have a duty to remedy that harassment).
[108] *See id.*

Warrantless Searches Using GPS Surveillance and the Role of the Fourth Amendment

By George S. Hodges and Kelly A. Hodges

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…."[1]

"A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[2]

"The needs of law enforcement…are quickly making personal privacy a distant memory. 1984 may have come a bit later than predicted, but it's here at last."[3]

United States v. Pineda-Moreno[4]

IN THE spring of 2007 Juan Pineda-Moreno, an Oregon resident, was arrested by agents of the Federal Drug Enforcement Administration ("DEA") and subsequently indicted for several possible drug-related activities. Utilizing a number of mobile tracking devices attached to his Jeep at various locations, DEA agents had continuously monitored the activities of Pineda-Moreno and several companions over the course of the almost four months, eventually leading the agents to a marijuana "grow site." A subsequent search of Pineda-Moreno's trailer located a large quantity of marijuana. At trial, Pineda-Moreno sought to exclude any evidence obtained through use of the tracking device, claiming that attachment of the system to his automobile while it was in his driveway without a warrant violated his Fourth Amendment rights. The lower court denied his motion to suppress. On appeal, the Court of Appeals for the 9th Circuit affirmed the lower court's determination, holding that the Pineda-Moreno did not have a "reasonable expectation of privacy" in and about his driveway and that there had been no Fourth Amendment violation

George Hodges is a partner with Hodges Walsh & Slater in White Plains, N.Y. He served as IADC President (2004-2005). He concentrates his practice in the areas of product liability, toxic tort, drug and medical devices and business litigation.

Kelly Hodges is a 2010 graduate of Virginia School of Law. She is awaiting admission to the New York State Bar and is associated with a New York City law firm.

United States v. Maynard[5]

In March 2007, Lawrence Maynard and Antoine Jones were indicted on a series of drug related charges. At trial, both individuals were convicted of distributing quantities of cocaine. Jones appealed his conviction, arguing in part against evidence that had been gathered by a joint police task force that had monitored his activities on a twenty-four/seven basis for four weeks, utilizing a GPS device that had been installed on his car without a warrant. In considering, and ultimately rejecting, the findings of

the Ninth Circuit in *Pineda-Moreno*, the District of Columbia Circuit Court of Appeals reversed the rulings of the trial court and the conviction of Jones, holding that under *United States v. Katz*[6] the use of the GPS device twenty-four hours a day over the course of a month constituted a search because it defeated Jones' reasonable expectation of privacy. Thereby, such surveillance required a warrant.

I. Introduction

Just as with virtually every other facet of our lives, continuing advancements in technology have created a new set of rules in the centuries old game of *Cops v. (alleged) Bad Guys.* Just as the planning and carrying out of complex criminal schemes has been significantly modernized in recent years through the use of internet sources, data bases, etc., so too have police investigative procedures in the continuing effort to stay one step ahead of the "perpetrators." This article will explore the now frequent use of Global Positioning System devices ("GPS") in surveillance of the day-to-day (and often week-to-week or even month-to-month) activities of individuals and whether privacy rights afforded by the Fourth Amendment to the U.S. Constitution are violated by such surveillance. The issue has been a major focal point in multiple federal and state court actions in recent years, resulting in a significant division of opinions and approaches, particularly among the judges of the Circuit Courts.

Despite the rash of decisions, articles, blogs and other discussions, the topic of the use of modern technology in the surveillance of actual and/or perceived criminals, the Supreme Court has not reviewed the issue of Fourth Amendment rights and unreasonable searches and seizures for more than 25 years. When the issue of police surveillance and subsequent arrest comes before the courts today, judges turn for guidance to opinions on technology issued in an era when Pong was the computer game of choice, 8-tracks provided our musical entertainment and "beepers" were the newest and most modern tool of surveillance. Back then, following the activities of individuals through devices was limited by the technology of the time to a battery operated radio transmitter sending out periodic signals to a radio transmitter which required personal monitoring; today the use of global positioning systems "yields … a highly detailed profile, not simply of where we go, but by easy inference, of our associations – political, religious, amicable and amorous to name only a few – and of the pattern of our professional and vocational pursuits."[7] Or, as *Wikipedia* so succinctly defines the GPS system and its uses: "a space- based global navigation satellite system … that provides reliable location and time information in all weather and at all times and anywhere on or near the Earth …."[8] Certainly today's surveillance methods are a far cry from the "beepers" considered and ruled upon by the Supreme Court in *U.S. v. Knotts*[9] and seemingly such systems are worthy of modern review and reconsideration of Fourth Amendment issues.

II. History

The core foundation for the majority of rulings on search and seizure issues in the past 40 years was the decision of the Supreme Court in *Katz v. United States*.[10] Katz was charged with transmitting wagering information between states by telephone in violation of federal wire communication statutes. Katz was convicted primarily due to the admission into evidence "of telephonic conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from where he had placed his calls."[11] The Court of Appeals for the Ninth Circuit had rejected the argument that use of electronic listening and recording devices had violated the defendant's Fourth Amendment Rights. In finding that Katz had been subjected to an unreasonable search and seizure and reversing his conviction, the Supreme Court emphasized:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[12]

Since the issuance of the decision in *Katz*, the most cited and relied upon portion of the opinion has been the "two prong test" set forth in Justice Harlan's concurring opinion:

> As the Court's opinion states, "the Fourth Amendment protects people, not places." The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place." My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[13]

Justice Harlan further explained the expectations of privacy to which an individual is entitled:

> "[T]hat one who occupies [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that his conversation is not being intercepted." *Ante*, at 352. The point is not that the booth is "accessible to the public" at other times, *ante*, at 352, but that it is a temporarily private place whose momentary occupants' expectation of freedom from intrusion are recognized as reasonable. Cf. *Rios v. United States*, 364 U.S. 253.[14]

Some sixteen years after delivering its opinion in *Katz*, the Supreme Court considered an issue of more "discrete" surveillance and evidence gathering in *United States v. Knotts*.[15] The facts in *Knotts* were relatively simple. Drug enforcement agents in Minnesota

believed that the defendants had manufactured a variety of controlled substances and that, as part of this operation, large amounts of chemicals used in manufacturing "illicit drugs" had been stolen and/or purchased from various facilities. The agents installed a radio transmitting beeper into a five gallon container of chloroform, which was then purchased by one of the suspected drug manufacturers. Police followed the individual with both visual surveillance and monitoring of the beeper resulting eventually in the obtaining of a warrant to search the premises where the surveillance beeper led them and the eventual conviction of the individuals involved. As the Supreme Court noted, "[t]he Eighth Circuit reversed the conviction, finding that the monitoring of the beeper was prohibited by the Fourth Amendment because its use had violated respondent's reasonable expectation of privacy, and that all information arrived after the location of the cabin was fruit of the illegal beeper monitoring."[16]

Upon review, the Supreme Court reversed the Eighth Circuit's decision and reinstated the conviction. Although the Court was unanimous in its holding, there were several separate opinions included within the decision, each of which would provide ample support and reasoning for future diverse approaches to and opinions on the use of surveillance equipment and applicability of the Fourth Amendment.

Initially, in delivering the majority opinion, Justice Rehnquist reaffirmed the court's holding in *Katz* and, more particularly the two "discreet questions" referred to in Justice Harlan's concurring opinion. These principles were discussed in *Smith v. Maryland*[17] and reaffirmed in *Knotts*,

> "Consistently with *Katz,* this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a `reasonable,' or a `legitimate expectation of privacy' that has been invaded by government action. This inquiry, as Mr. Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has `exhibited an actual (subjective) expectation of privacy,' — whether, in the words of the *Katz* majority, the individual has shown that `he seeks to preserve [something] as private.' The second question is whether the individual's subjective expectation of privacy is `one that society is prepared to recognize as 'reasonable,' *id.*, at 361 — whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is `justifiable' under the circumstances."[18]

The Court in *Knotts* reiterated the longstanding rule that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,"[19] emphasizing that visual surveillance in and of itself along the route of travel would have revealed the same facts to the police and that "nothing in the Fourth Amendment prohibited the police from augmenting the sensory

faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[20]

This is equally true as to the exterior or the undercarriage of a vehicle since "the undercarriage is part of the car's exterior, and as such, is not afforded a reasonable expectation of privacy."[21]

Either intentionally or unintentionally, Justice Rehnquist left open the possibility that the Court might have to re-visit its finding in *Knotts* should technology improve so that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision."[22] The court seemingly left the door open for future reconsideration, stating, "[i]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[23]

However, the Court summarily rejected the inference by the respondent of impropriety on the part of the police in making use of advances in technology as a means of detecting crime stating that: "we have never equated police efficiency with unconstitutionality, and we decline to do so now."[24]

III. Division Among the Courts in Recent Years

As the "beeper at the core of the Knotts was replaced by the GPS system and other modern surveillance devices and the methods and means of keeping track of the daily, weekly and monthly activities of suspects became more sophisticated, it might be argued that the poster child of the "dragnet-type law enforcement practices" envisioned by Justice Rehnquist had become a reality. In fact, the GPS has become a focal point for many, if not most, police surveillance efforts and, not surprisingly has resulted in a multitude of Fourth Amendment related decisions in recent years in both federal and state courts.

A. United States v. Pineda-Moreno

As discussed in the introduction, drug enforcement agents suspected Pineda-Moreno and several of his companions to be marijuana growers based on the observations of grocery purchases common to the manufacturing of illegal substances. On separate occasions, DEA agents attached tracking devices to the underside of Pineda-Moreno's vehicle. Four of the devices were attached while the vehicle was parked on a public street in front of the Pineda-Moreno home. One of the installations took place in a public parking lot. The other two devices were installed while Pineda-Moreno's car was parked in his driveway, a few feet from the side of his trailer. The information gathered from the mobile tracking devices over the course of more than four months resulted in DEA agents pulling over the car and the subsequent arrest of three individuals in the Jeep premised upon "violations of immigration laws."[25] A grand jury later added counts of conspiracy to manufacture marijuana and manufacturing marijuana. Pineda-Moreno eventually entered a conditional guilty plea but reserved the right to appeal the denial of his motion to suppress use of

any evidence related to or emanating from the use of the GPS devices.

The crux of Pineda-Moreno's argument was directed to the installation of the devices while his car was parked in the driveway adjacent to his home. The court summarily rejected this argument, holding that:

> In sum, Pineda-Moreno cannot show that the agents invaded an area in which he possessed a reasonable expectation of privacy when they walked up his driveway and attached the tracking device to his vehicle. Because the agents did not invade such an area, they conducted no search, and Pineda-Moreno can assert no Fourth Amendment violation.[26]

In other words, since the defendant had not supplemented his driveway with "special features" such as enclosures, barriers on the gates, "'no trespassing" signs and "did not take steps to exclude passersby from his driveway,"[27] he could not claim a reasonable expectation of privacy in it, regardless of whether a portion of the driveway was located within the curtilage of his home. The logic that the nature and number of embellishments and security devices to the driveway somehow should determine the applicability of the Fourth Amendment, became a focal point in an unsuccessful petition for rehearing en banc several months later.

The three member Ninth Circuit panel that originally heard the appeal was unanimous in its decision to deny Pineda-Moreno's motion to suppress. The defendant then petitioned for a rehearing of the issue before the entire court. As the petition "failed to receive a majority of the votes of the non-recused active Judges" it was denied in a simple three paragraph decision.[28] However, Chief Judge Kozinski, along with four other Judges, dissented from the denial of rehearing. In a strongly worded, often sarcastic and belittling dissenting opinion, Chief Judge Kozinski criticized and rejected the original opinion of his colleagues finding that:

> The needs of law enforcement, to which my colleagues seem inclined to refuse nothing, are quickly making personal privacy a distant memory. 1984 may have come a bit later than predicted, but it's here at last.[29]

The dissent relied quite heavily on Justice Rehnquist reference to "twenty-four hour surveillance" in *Knotts* and "dragnet-type law enforcement practices,"[30] warning that:

> I don't think that most people in the United States would agree with the panel that someone who leaves his car parked in his driveway outside the door of his home invites people to crawl under it and attach a device that will track the vehicle's every movement and transmit that information to total strangers. There is something creepy and un-American about such clandestine and underhanded behavior.[31]

Judge Kozinski seemed equally concerned with what the future might bring, warning that "[i]n determining whether the tracking devices used in

Pineda-Moreno's case violate the Fourth Amendment's guarantee of personal privacy, we may not shut our eyes to the fact that they are just advance ripples to a tidal wave of technological assaults on our privacy."[32]

A petition for certiorari was filed in November 2010, asking the Supreme Court of the United States to review the Ninth Circuit's decision.[33] As of publication the Supreme Court has not indicated whether it will grant certiorari.

B. United States v. Maynard

The applicable portions of the decision in this matter actually apply to and resulted in reversal of a conviction of Antoine Jones, a co-defendant with Lawrence Maynard. As with many of the decisions relating to searches and seizures, this case involved alleged narcotic violations and surveillance methods utilized by the authorities. Jones argued that the police had violated the Fourth Amendment through "unreasonable searches," which involved tracking his movement twenty-four hours a day for four weeks with a GPS device they had installed without a valid warrant.[34] More specifically, Jones argued that under the decision in *Katz* the GPS device violated his "reasonable expectation of privacy" and that it constituted a search subject to the reasonableness required by the Fourth Amendment.[35]

In agreeing with the substance of the contentions raised on behalf of Jones, the circuit court found that the decision in *Knotts* was not controlling and pointed out the reservation by the Supreme Court in *Knotts* of the question whether a warrant would be required in a case involving "twenty-four hour surveillance" and "dragnet-type law enforcement practice.[36] More specifically, Circuit Judge Ginsburg, writing the opinion for the unanimous panel, found:

> In short, *Knotts* held only that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it.[37]

The court specifically distinguished the decision of the Ninth Circuit in Pineda-Moreno pointing out that the other matter the defendant had not argued - that the prolonged surveillance by means of a monitoring device - constituted a search. The court found a significant difference between the use of the GPS device on a twenty-four hour per day basis over an extended period of time and "normal surveillance," since no argument could be made that each and every act or movement of an individual could be recorded over the course of an entire month using routine surveillance:

> Here the police used the GPS device not to track Jones's "movements from one place to another," *Knotts*, 460 U.S. at 281, but rather to track Jones's movements twenty-four hours a day for twenty-eight days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place.[38]

Utilizing the two-prong test discussed in *Katz*[39] the court held that "[w]hether an expectation of privacy is reasonable depends in large part upon whether that expectation relates to information that has been 'expose[d] to the public.'"[40] The court thereafter held that "the information the police discovered in this case—the totality of Jones's movements over the course of a month—was not exposed to the public."[41] The court noted that "[i]n considering whether something is "exposed" to the public as that term was used in *Katz* we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do."[42]

After an extensive discussion of the expectations of privacy to which an individual is entitled, Justice Ginsburg found:

> Applying the foregoing analysis to the present facts, we hold the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[43]

Finally, the Court in *Maynard* had some "words of wisdom" for its brethren in the other Circuit that disagreed with its holding, stating, "[t]he federal circuits that have held use of a GPS device is not a search were not alert to the distinction drawn in *Knotts* between short-term and prolonged surveillance …."[44]

As with the decision of the Ninth Circuit in *Pineda-Moreno*, a request was filed (this time by the Justice Department) for a full Appeals Court to review the issues in Maynard, but the Judges declined to do so by a five to four vote.[45] A petition for certiorari to the United States Supreme Court was filed, but summarily denied.[46]

C. Other Recent Federal decisions

The findings of the D.C. Circuit in *Maynard* certainly appear to be an exception to the holdings of the Federal District Courts in recent years, most of which echo the holding in *Pineda-Moreno* that *Knotts* is applicable today and that modern tracking devices utilized over extended periods do not constitute fourth Amendment violations.

- **United States v. Jesus-Nunez**[47]

  The defendant was a suspected drug supplier. GPS systems were attached to his cars while parked on a public street on two separate occasions. One GPS was in place for approximately eleven months, the other for approximately ten months. The systems tracked the date, time and precise locations of each stop of the car. The court denied the motion to suppress the evidence obtained

through the GPS systems citing the decision in *Knotts* as being directly on point. The opinion openly expressed concern for the duration of the GPS tracking and referenced commentary of Justice Rehnquist's in *Knotts* concerning twenty-four hour surveillance without knowledge or supervision. In seemingly calling for the Supreme Court to revisit this issue, District Judge Sylvia Rambo stated that "the court does not believe that it is in the position to rewrite constitutional principles long established by the Supreme Court because of the changing landscape of technology. This is the province either of Congress or the higher courts; it is this court's duty to apply precedent to the facts."[48]

- **United States v. Burton**[49]

  In accepting that *Knotts* was controlling, the court rejected the contention of an accused drug dealer that evidence obtained through the use of GPS devices over an extended period of time should be precluded holding that there was no reasonable expectation of privacy so long as a motor vehicle was being used on public streets.

- **Morton v. Nassau County Police Department**[50]

  A civil action was brought pursuant to 42 U.S.C. §1983. Morton claimed damages from the placement of a GPS transmitter on her automobile and the subsequent tracking of the vehicle, which ultimately resulted in the arrest of accused burglar driving plaintiff's vehicle. The court found that the use of the GPS device was not an unreasonable search or seizure in violation of the Fourth Amendment, relying heavily on the Supreme Court's decision in *Knotts*.

- **United States v. Sparks**[51]

  This decision constitutes perhaps the most thorough and up-to-date consideration of the issues arising from the use of modern technology, including GPS devices, and the applicability of *Katz* and *Knotts* several decades later. Sparks involved the attaching of a GPS device to Sparks' vehicle, based on the FBI's suspicion that Sparks had committed several bank robberies and planned to commit even further robberies. The device was affixed in the early morning hours of the day prior to a robbery while the car was parked in an open air lot used by tenants of several multi-unit residential buildings. The court utilized the two-prong test established in from *Katz* in determining whether the installation of the GPS device on the car and the monitoring of the location of the car infringed upon reasonable expectations of privacy. After finding that the FBI agents had not invaded any constitutionally protected area within Sparks' dwelling or curtilage and restating earlier decisions that motor vehicles are entitled to a significantly

diminished expectation of privacy, the court determined that "[b]ecause Sparks had no reasonable expectation of privacy either in the shared parking lot or in the exterior of his vehicle, the placement of the GPS device on the vehicle cannot be considered a search or seizure."[52] The Court also rejected Sparks argument "that the aggregate of his travels are entitled to more constitutional protection than his individual trips," stating that it was "unwilling, and unable, to extend the reach of the Fourth Amendment that far."[53]

D. Recent State Court Decisions

The use of modern tracking devices has not been limited to federal jurisdictions, but has also come up at discussion in multiple criminal cases passing through the state courts. As a general rule, the state courts have been more willing to limit and/or suppress the use of GPS data obtained without a warrant. In many instances, those courts have relied on the applicable state constitution, rather than the U.S. Constitution, as the basis for the protection against warrantless searches.

- **People v. Weaver**[54]

  A GPS tracking device had been placed underneath a street-parked van and remained in place for 65 days constantly monitoring the position of the van. No warrant had been obtained for use of the GPS surveillance while "it is not clear from the record why defendant was placed under electronic surveillance," he was charged with burglary related crimes and was eventually convicted premised in part upon use of the data obtained from the GPS surveillance. The Court of Appeals of New York held that the search obtained through the GPS was illegal and reversed the conviction. While emphasizing that its findings were premised on state law rather than federal, the majority in the four-to-three decision distinguished modern technology from that which the Supreme Court discussed in *Knotts*:

  > Here, we are not presented with the use of a mere beeper to facilitate visual surveillance during any single trip. GPS is a vastly different and exponentially more sophisticated and powerful technology that is easily and cheaply deployed and has virtually unlimited and remarkably precise tracking capability. Constant, relentless tracking of anything is now not merely possible but entirely practicable, indeed much more practicable than the surveillance conducted in Knotts.[55]

- **Foltz v. Commonwealth**[56]

  David Foltz was a registered sex offender on probation who was suspected by the police in a series of sexual assaults. Based on the location of a series of sexual assaults in the vicinity of where Foltz was employed, the police attached a GPS system to one of his work vehicles

without a warrant and without permission from the employer. After another sexual assault took place, the police checked the GPS log and found that Foltz's vehicle had been parked a short distance from the scene of the attack at the time it occurred. The police then began a visual observation of Foltz and caught him in the act of assaulting another victim. At trial, Foltz moved to suppress all evidence collected after the police began to track him via the GPS system. In denying the motion to suppress, the court recognized the warnings in *Knotts* about "dragnets" and "mass surveillance" but found them inapplicable to the facts in this case. The court did apply a two-prong *Katz* test but found that defendant failed both parts since there was no subjective expectation of privacy in driving a work van down the street and no reasonable expectation of privacy for vehicles on public streets. The Court of Appeals of Virginia soon after ruled that it would rehear the case en banc and the mandate entered by the panel of judges was stayed pending the full court's ruling.[57]

- **State v. Jackson**[58]

The court discussed at length why the use of a GPS device to monitor Jackson's activities did not equate to merely following him on the road and how the GPS device constituted a significant intrusion into private affairs. Since "citizens of this State have a right to be free from the type of governmental intrusion that occurs when a GPS device is attached to a citizen's vehicle regardless of reduced privacy expectations due to advances in technology" and that a warrant is required for installation of GPS devices.[59] Unfortunately, this was the extent of the good news for Jackson, as the court also found that the police had obtained valid warrants premised upon appropriate affidavits and that the evidence obtained from the GPS systems was appropriate. Although it created a great deal of positive language to be used by others, Jackson's conviction and sentence were affirmed.

---

[1] U.S. CONST. amend. IV.
[2] United States v. Knotts, 460 U.S. 276, 281 (1983).
[3] U.S. v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010), *rehearing en banc denied*, 617 F.3d 1120, 1121(9th Cir. 2010) (Kozinski, J, dissenting).
[4] 591 F.3d 1212 (9th Cir. 2010).
[5] 615 F.3d 544 (D.C. Cir. 2010).
[6] 389 U.S. 347 (1967).
[7] People v. Weaver, 909 N.E.2d 1194, 1199 (N.Y. 2009).
[8] *Global Positioning System*, Wikipedia, http://en.wikipedia. org/wiki/Gps (last visited Dec. 20, 2010).
[9] 460 U.S. 276 (1983).
[10] 389 U.S. 347 (1967).
[11] *Id.* at 348.
[12] *Id.* at 352 (citations omitted).
[13] *Id.* at 361 (Harlan, J., concurring).
[14] *Id.*
[15] 460 U.S. 276 (1983).
[16] *Id.* at 279-80.
[17] 442 U.S. 735 (1979).
[18] 460 U.S. at 280-81 (quoting Smith v. Maryland, 442 U.S. 735, 740-41 (1979)) (citations omitted).
[19] *Id.* at 281.

[20] *Id.* at 282.
[21] United States v. Rascon-Ortiz, 994 F.2d 749, 754 (10th Cir. 1993).
[22] 460 U.S. at 283 (citing brief for the respondent).
[23] *Id.* at 284.
[24] *Id.*
[25] 591 F.3d 1212, 1214 (9th Cir. 2010).
[26] *Id.* at 1215 (citations omitted).
[27] *Id.*
[28] United States v. Pineda-Moreno, 617 F.3d 1120, 1120-21 (9th Cir. 2010).
[29] *Id.* at 1121 (Kozinski, J., dissenting).
[30] 460 US at 284.
[31] *Id.* at 1126.
[32] *Id.* at 1125.
[33] United States v. Pineda-Moreno, 591 F.3d 1212, *petition for cert. filed sub nom.*, No. 10-7515 (U.S. Nov. 10, 2010).
[34] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
[35] *Id.* at 555.
[36] *Id.* at 556 (quoting United States v. Knotts, 460 U.S. 276, 284 (1983)).
[37] *Id.* at 557 (citations omitted).
[38] *Id.* at 558.
[39] 289 U.S. 351, 361 (1967) (Harlan, J., concurring).
[40] 615 F.3d at 558 (quoting *Katz*, 289 U.S. at 351).
[41] 615 F.3d at 558.
[42] *Id.* at 559.
[43] *Id.* at 560.
[44] *Id.* at 564.
[45] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *rehearing en banc denied sub nom.*, United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010).
[46] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *cert. denied sub nom.*, Maynard v. United States, No. 10-7102, 2010 WL 4156203 (Nov. 29, 2010).
[47] No. 1:10-CR-00017-01, 2010 WL 2991229 (M.D. Pa. July 27, 2010).
[48] *Id.* at *4.
[49] 698 F. Supp.2d 1303 (N.D. Fla. 2010).
[50] No.05-CV-4000 (SJF) (AKT), 2007 WL 4264569 (E.D.N.Y. Nov. 27, 2007).
[51] No. 10-10067-WGY, 2010 WL 4595522 (D. Mass. Nov. 10. 2010).
[52] *Id.* at *6.
[53] *Id.* at *8.
[54] 909 N.E.2d 1194 (N.Y. 2009).
[55] *Id.* at 1199.
[56] 698 S.E.2d 281 (Va. Ct. App. 2010).
[57] 699 S.E.2d 522 (Va. Ct. App. 2010).
[58] 76 P.3d 217 (Wash. 2003).
[59] *Id.* at 24.

Sealing Your Settlement Agreement from the Public Eye

By Christopher R. Christensen and Evan M. Kwarta

IN TWO previous editions of the IADC Privacy Project, William B. Crow examined how and when settlement agreements that require court approval can be kept under seal. In 2004, Mr. Crow examined the arguments in favor of, and in opposition to, sealing settlement agreements, as well as specific efforts by certain jurisdictions to prevent settlement agreements from being filed under seal (hereinafter "Crow I"). In 2007, Mr. Crow examined a variety of hypotheticals involving sealed settlement agreements, and the legal and ethical considerations attorneys must confront when attempting to shield settlement agreements from the public eye (hereinafter "Crow II"). Both articles cautioned that parties, particularly defendants, should not expect that judges will accept settlement agreements for filing under seal, and advised that to the extent litigants hope to shield those agreements from the public, they must make every effort to refrain from entering into settlement agreements that require judicial approval. That advice remains the same today – even where the parties to a settlement agreement agree to keep that settlement confidential, they should not expect it to remain so where the settlement agreement requires judicial approval.

Since Mr. Crow's articles were published, the movement among certain state legislatures, judges and plaintiffs' attorneys to prevent sealed settlement agreements has become even stronger. This article focuses on forums that embrace the movement against confidentiality, and examines recent exemplary cases, including the success of arguments commonly made in support of motions to seal settlement agreements.

Christopher R. Christensen is a partner with Condon & Forsyth LLP in New York City. He concentrates his practice in the areas of complex aviation, product liability and commercial litigation.

Evan M. Kwarta is an associate who works in the same practice group.

I. Additional Forums that Disfavor Sealed Settlement Agreements

In 2004, Mr. Crow carefully reviewed certain forums that employ "Sunshine Acts" or similar rules that prohibit or restrict the sealing of any court records, including settlement agreements, when those records contain information related to a so-called "public hazard."[1] Crow I noted that when defending cases in any of those forums, parties must be prepared for the probability that their settlement agreement, even if intended to be kept confidential, could be revealed to the public.[2] That advice is applicable to several additional forums identified below.

State courts in South Carolina, much like their federal counterparts, are specifically prohibited from approving settlements that are conditioned upon being filed under seal.[3] State courts in Louisiana and Arkansas prohibit

confidentiality provisions in any contracts, including settlement agreements, where those contracts relate to public[4] or environmental[5] hazards, respectively.

Like Texas, the state of Washington has made a specific legislative finding that the public health is promoted by a prohibition of confidentiality provisions that conceal matters that relate to public health.[6] And under Virginia law, protective orders entered in personal injury and wrongful death cases cannot prohibit attorneys from conferring with other attorneys, who are not involved in the case in which the protective order was entered, but who are involved in similar or related matters.[7] Counsel defending cases in any of these jurisdictions should be aware that each of these rules reflects a policy preference in favor of transparency and against sealed settlement agreements. Accordingly, in those jurisdictions, if a settlement agreement requires judicial approval, it is unlikely to be accepted for filing under seal.

This policy preference has made it to the halls of the U.S. Congress where three "Sunshine in Litigation" bills[8] are pending that would modify the Federal Rules of Civil Procedure to (1) prohibit federal courts from entering Rule 26(c) protective orders and orders sealing a settlement agreement, where such orders would restrict the disclosure of information relevant to the public health or safety; (2) dissolve all protective orders (except those that sealed a settlement agreement) upon the entry of final judgment, unless the court makes a separate finding that the protective order should remain in effect; and (3) prohibit federal courts from enforcing the terms of a settlement agreement that precludes the parties from revealing the fact or terms of a settlement (other than the amount of money paid), or precludes the dissemination of evidence from that case if the case involved matters relating to the public health or safety.

"Sunshine" amendments to the Federal Rules of Civil Procedure have been proposed and rejected before.[9] Moreover, because these particular bills were opposed both by the ABA and the Judicial Conference of the United States they are not likely to become law. However, the continued proposal of "Sunshine" acts in the U.S. Congress[10] and the increasing number of jurisdictions with "Sunshine" acts,[11] coupled with a growing preference among judges for open settlement agreements, should give pause to attorneys who either believe that their client's settlement agreement is certain to remain confidential or who factor the need for confidentiality into their settlement negotiations. That growing preference among judges is encapsulated in the recent case law detailed below.

II. The Judicial Movement Against Sealed Settlement Agreements

Before examining recent case law concerning judicially approved sealed settlement agreements, it is worth examining the landscape in which the need for judicial approval of settlement agreements arises and how that need factors into a judge's decision as to whether to accept a settlement agreement for filing under seal. This article will primarily address cases decided subsequent to Crow II because Mr.

Crow's articles deftly addressed cases decided in 2007 and before.

Very few settlement agreements require judicial approval. A Federal Judicial Center study[12] of federal cases with sealed settlement agreements revealed that sealed settlement agreements are filed in approximately four-tenths of one percent of all federal cases.[13] The Federal Judicial Center also concluded that less than two-tenths of one percent of all cases both had sealed settlement agreements[14] *and* arguably were related to the public health or safety.[15] Ultimately, the Federal Judicial Center concluded that the number of cases with sealed settlement agreements was too small to necessitate a change in the Federal Rules of Civil Procedure.[16]

Of that four-tenths of a percent of cases that had sealed settlement agreements, a plurality of those cases were ones that typically require judicial approval, such as those involving a minor, or actions filed pursuant to the Fair Labor Standards Act (hereinafter the "FLSA"), where, particularly among FLSA cases, courts have found that the public interest in open access to judicial records can outweigh the parties' need for privacy.[17] The growing reluctance among judges to seal FLSA cases is discussed below.

III. The Refusal to Seal FLSA Cases

A primary concern among those opposed to sealed settlement agreements is that confidentiality will conceal from the public certain vital information in which the public has an interest. In other words, certain settlement agreements serve not just a private function, but also a public function.[18] Judicial construction of plaintiffs' FLSA rights has similarly recognized a public-private interest because, courts state, the FLSA was intended not simply to compensate employees for lost wages, but also to publicly punish employers for violating the FLSA, and to put other employees on notice that they may have a claim against their employer.[19] Accordingly, courts have found that sealing FLSA settlement agreements thwarts the public-private objective of the FLSA by permitting employers to hide their violations from the public and their employees.[20] Judicial analysis of the balance between the public and private interests that arise in FLSA cases, therefore offers an effective window into the challenges judges confront with sealed settlement agreements, as well as how attorneys can expect motions to seal settlement agreements to be resolved.

In recent cases analyzing motions to seal FLSA settlement agreements, courts have considered and rejected most of the common arguments defendants make in favor of sealing settlement agreements. For instance, defendants frequently argue that confidentiality plays a vital role in settlement negotiations and that settlement agreements often cannot be reached without the assurance that the settlement terms will not be disclosed.[21] While courts are mindful that they must balance the harm that disclosure could wreak on the settlement process against the presumption of access to judicial records,[22] courts typically have been persuaded that the public interest in access to FLSA records, and judicial records generally, is superior to defendants' amorphous arguments

regarding the nature of settlements.[23] This should be particularly alarming because almost all motions to seal FLSA settlement agreements are unopposed; courts are denying these motions for reasons that they come up with on their own.

Courts analyzing motions to seal FLSA settlement agreements also have rejected other common, but non-specific arguments made by defendants, such as the fact that the parties privately agreed to a confidentiality provision and they should be entitled to the benefit of their bargain;[24] that unsealing a settlement agreement may have a chilling effect on future, similar settlement negotiations;[25] that businesses are entitled to keep their legal proceedings private;[26] and that disclosure of settlement agreements would prompt additional litigation and make the defendant a target for similar but frivolous lawsuits.[27]

Plaintiffs often favor sealing FLSA settlement agreements as well, in the hope that their personal and private information, and the settlement amount, will not become public.[28] Yet courts deciding recent FLSA cases have found that the plaintiff's personal privacy interests are ultimately subordinate to both the public-private nature of FLSA claims, as well as the need for judicial transparency.[29]

Courts often reject these common arguments while offering the parties the opportunity to withdraw their settlement agreement,[30] essentially challenging the parties to prove how important confidentiality really is. Having already expended substantial resources in order to reach a settlement, and faced with the possibility of a trial, few parties withdraw their settlement.

In short, courts considering motions to seal FLSA settlement agreements are likely to reject the common and non-specific arguments that parties ordinarily make in support of these motions. While courts have not given any particularly helpful examples of what sorts of interests might tip the balance in the favor of parties seeking to file a settlement agreement under seal (apart from the potential harm that could result from the release of trade secrets or other proprietary information[31]), it appears that in order to prevail on these motions, the parties must present the court with specific and significant harms that would result from unsealing.[32]

IV. Public Hazards and High-Profile Cases

The classic case involving so-called "public hazards" is a product liability case, and the movement against sealed settlement agreements in those cases is strong. For instance, in *Perreault v. The Free Lance-Star*,[33] a defendant pharmaceutical company settled four wrongful death claims arising from an allegedly contaminated liquid solution that was used in the decedents' open heart surgeries. Pursuant to Virginia law requiring judicial approval of wrongful death settlement agreements,[34] the parties jointly moved the trial court for an *in camera* inspection, and approval, of the settlement agreements.[35] Several news-papers intervened, objecting to the *in camera* review, and the parties moved to file the settlement agreements under seal.[36] The case ultimately made its way

to the Virginia Supreme Court, which concluded that where parties are required to obtain court approval of their settlement agreements, a public interest in seeing that the judiciary is fairly and honestly administering justice attaches, and outweighs the parties' interests in keeping settlement agreements sealed.[37] The court then went a step further and placed the burden in motions to seal settlement agreements squarely on parties seeking to seal records, requiring them to put forth facts upon which a court could make specific factual findings that support sealing court records, rather than placing the burden on intervenors to demonstrate how they would be harmed if the records were maintained under seal.[38]

High profile cases arguably involving the public interest, or so-called "public hazards," can also attract judicial scrutiny of sealed settlement agreements even in jurisdictions without a clearly stated legislative or judicial preference for open settlements. In these jurisdictions, the common law regarding protective orders governing discovery can be instructive in predicting whether a court would allow parties to file a settlement agreement under seal, because the same motivation applies to both the prohibition of protective orders in cases relating to public hazards and the prohibition of sealed settlement agreements.

For instance, in *Verni v. Lanzaro*,[39] a mother brought suit on her own behalf and her infant daughter's behalf after they were injured by a drunk driver who became intoxicated at a New York Giants football game. After settling with some defendants, the plaintiff entered into a separate settlement agreement with Aramark, the concession operator at Giants Stadium.[40] The trial court granted a motion to seal the Aramark settlement agreement, but Public Citizen, a self-described public interest group focused on protecting public health and safety,[41] intervened and moved to unseal it.[42] The parties opposed the motion, the plaintiff on the grounds that the seal protected the information of a minor, and Aramark on the grounds that the seal furthered the public interest in settlements.[43] The trial court denied Public Citizen's motion.

The appellate court reversed, finding that the public interest in whether alcohol could be safely dispensed at a football game outweighed the plaintiff's desire for privacy.[44] The court applied the analysis from *Hammock v. Hoffman-La-Roche, Inc.*,[45] a case where Public Citizen also intervened. In *Hammock*, the New Jersey Supreme Court spelled out guidelines for when court records that potentially affect the public health and safety should remain under seal and applied those guidelines to discovery that was attached to summary judgment motions.[46] In doing so, the New Jersey Supreme Court did not specifically refer to settlement agreements, but did analyze "Sunshine" acts such as those in Florida, Texas, Virginia and New York, that are discussed above. The *Verni* court's application of the principles announced in *Hammock* highlights the interplay between the rules governing protective orders and those concerning sealed settlement agreements, and suggests that the courts' analysis of protective orders in cases where the public health is arguably at issue can be instructive in forming arguments in support of motions to seal settlement agreements.[47]

Even high-profile cases that do not concern matters of public health can draw judicial scrutiny. In *Schoeps v. Museum of Modern Art*,[48] plaintiffs claimed that two world-famous New York art museums owned Picassos taken from plaintiffs' ancestors by the Nazis, and that the museums had turned a blind eye to the theft.[49] The museums vigorously denied the accusations, and the case received a great deal of media attention.[50] On the morning that trial was scheduled to start, the parties reached an agreement allowing the museums to keep the paintings, but the parties refused to disclose the term of the settlement to the public.[51] The court urged the parties to submit the agreement under seal for the court's review – which they did – and convinced the museums to drop their objection to public disclosure of the settlement agreement, but the plaintiffs refused to relent.[52] In a published opinion, the court strongly criticized the parties for agreeing to a confidential settlement in such a high-profile case.[53] But constrained by rule and precedent, the court concluded it could not disclose the terms of the settlement.[54] Although the agreement remains under seal, the fact that the court felt it necessary to publish an opinion that did nothing but urge the parties to disclose the terms of their settlement speaks volumes about the trend among some judges toward greater transparency.

In perhaps the most highly publicized settlement since the last edition of the Privacy Project, the trial court *In re Sept. 11th Litigation*, decided not only to remove the seal, but also to disclose the settlement's terms, eviscerating the parties' ability to successfully pursue the issue on appeal.[55]

The litigation arose out of a claim by certain multi-national property insurers and property owners that a group of airlines, airport security companies, an aircraft manufacturer, and the municipal owner of the departure airport were responsible for the property destruction that occurred as a result of the 9/11 terrorist attacks. Most of the plaintiffs settled with some of the defendants, and the settling parties jointly moved the court to approve their settlement, and maintain under seal information relating to (1) the total settlement amount; (2) the amount that each defendant was paying; and (3) the amount that each plaintiff was receiving (collectively, the "settlement agreement information").[56] The parties even secured a recommendation from the former federal judge who mediated their settlement, who advised the court that he believed the settlement agreement information should remain under seal.[57] The motion to seal was initially unopposed and was granted.[58] However, the court noted its reluctance in maintaining the settlement agreement information under seal, stressed the public importance of the case, and reserved its right to revisit its ruling should a motion for reconsideration be presented.[59]

Nearly three months later, the *New York Times* (hereinafter "the *Times*") intervened, moved to unseal the settlement agreement information.[60] The defendants argued that they had reasonably relied on the sealing order, and that the *Times* needed to show some compelling need justifying disclosure in order to unseal the settlement agreement information.[61] The court found that the defendants could not have reasonably

relied on the sealing order because the court had reserved its right to reconsider its decision, and therefore rejected that argument.[62] The defendants also argued that unsealing the settlement agreement information would have a chilling effect on the defendants' attempt to settle unresolved property damage cases, and that it would cast them in a false light by suggesting that the amounts they were paying to settle the cases meant that they were responsible for the 9/11 attacks.[63] The court was unsympathetic to these arguments because, as in most cases, the parties intended to go forward with their settlement agreement regardless of how the court resolved the motion to unseal.[64] However, the court left under seal the amount each settling plaintiff was to receive,[65] a peculiar result considering that the plaintiffs, most of which were multi-national insurance companies or sizable domestic businesses, arguably had a lesser interest in maintaining the amount of their settlement proceeds under seal than did the defendants with respect to the amounts that they paid. Moreover, the court took the unusual step of not simply vacating its prior order maintaining the confidentiality of the settlement agreement, but of publicizing the details in an order issued that same day approving the settlement.[66]

V. Conclusion

The bottom line when it comes to keeping settlement agreements under seal is that if the settlement requires judicial approval, it is unlikely to remain confidential. This is particularly true of high-profile cases, ones that arguably involve a so-called "public hazard," or ones in a jurisdiction that has a "Sunshine" act or similar rule disfavoring or prohibiting sealed settlement agreements. Parties also can look to cases involving public hazards and protective orders over discovery to help predict whether their settlement agreement is likely to be accepted for filing under seal in their jurisdiction. To the extent that defendants are able to convince courts to maintain settlement agreements under seal, they probably will have to do so by referring the court to specific prejudice that one or both parties will incur absent confidentiality. Arguments relying on vague assertions as to the parties' expectation of confidentiality, the importance of maintaining private information, the chilling effect unsealed settlement agreements will have on future settlement negotiations, or the potential that a defendant could become a target for future frivolous lawsuits, are increasingly likely to be rejected without a showing of a more specific harm. Ultimately, whenever attorneys negotiate a settlement agreement, they need to be mindful that although it does not appear that sealed settlement agreements will be outlawed completely any time soon, judges increasingly are taking matters concerning sealed settlement agreements into their own hands.

---

[1] Crow I identified Florida's "Sunshine in Litigation Act," FLA. STAT. § 69.801, which prohibits a court from sealing any record or information that has the effect of concealing a "public hazard." "Public hazards" are typically defined as products, persons or procedures that have caused, or are likely to cause, injury. *See id.* The article also identified (1) Texas Rule of Civil Procedure

76a, which creates a presumption that court records are open to the public that can be overcome only by a showing of a specific, serious, and substantial interest that outweighs both the presumption and any probable adverse effect that sealing the record will have on the public health and safety; (2) Uniform Rules for New York State Trial Courts § 216.1 that prohibits the sealing of any court record without a court first issuing a written finding of good cause that outweighs the presumption of public access to court records; and (3) Local Civil Rule 5.03 of the United States District Court, District of South Carolina that specifically prohibits any settlement agreement from being filed under seal.

[2] *See* Crow I at 112.

[3] S.C. R. CIV. P. 41.1. South Carolina also requires that all settlement agreements to which a minor is a party and that are in excess of $25,000 be approved by a court. *See* S.C. CODE § 62-5-433. The combination of these two rules means that any settlement with a minor in excess of $25,000 cannot be filed under seal.

[4] LA. CODE CIV. PROC. § 1426.

[5] ARK. CODE § 16-55-122.

[6] WASH. REV. CODE § 4.24.601. Despite this legislative finding, this provision of Washington code has not been applied in any cases.

[7] VA. CODE § 8.01-420.01.

[8] Two of the bills are pending in the House (H.R. 5419, 111th Cong. (2010), and H.R. 1508, 111th Cong. (2009)), and one bill is pending in the Senate (S. 537, 111th Cong. (2009)). S. 537 and H.R. 1508 are identical. H.R. 5419 is nearly identical to S. 537 and H.R. 1508, except that it contains additional clauses relating to civil actions, wherein the pleadings state facts relevant to public health or safety. The difference is semantic, however, as the other two bills contain fewer, but similar, clauses and the judicial interpretation of H.R. 5419 would not likely be affected by its additional clauses.

[9] *See Sunshine in Litigation Act of 2009: Hearing Before the H. Subcomm. on Commercial and Admin. Law*, 111th Cong. 60 (2009) (statement of Judge Mark R. Kravitz on behalf of the Rules Committees of the Judicial Conference of the United States) (hereinafter "Kravitz Statement").

[10] A "Sunshine in Litigation" bill was first introduced to Congress 1991. *See id.* at 60.

[11] *But see* Crow I at 112 (noting that twelve states have considered but rejected similar legislation).

[12] *See Sealed Settlement Agreements in Federal District Court*, Federal Judicial Center, 3 (2004) (hereinafter the "FJC Report"). The FJC Report examined cases decided in 2001 and 2002.

[13] In approximately one quarter of those cases, the settlement agreement was not initially filed with the court and was only filed under seal later because it was attached as an exhibit to a motion to enforce the settlement agreement, or as an exhibit to an otherwise sealed proceeding or transcript. *See id.* at 6. Those cases are not addressed here.

[14] Kravitz Statement, *supra* note 9, at 65.

[15] FJC Report, *supra* note 12, at 8. The FJC Report considered the following types of cases as related to public health or safety: (1) environmental; (2) product liability; (3) professional malpractice; (4) public-party defendant; (5) death or serious injury; and (6) sexual abuse.

[16] Kravitz Statement, *supra* note 9, at 65-67. The FJC also noted that a rule prohibiting sealed settlement agreements was unnecessary because in 97% of the cases identified in the FJC Report, *supra* note 12, the complaint or some other document detailing the nature of any potential public hazard was not sealed. *See id.*; FJC Report, *supra* note 12, at 6-7. This finding is critical because a common argument in opposition to permitting the filing of sealed settlement agreements is that they conceal the nature of potential public hazards. *See, e.g.*, Crow I, at 107; *Sunshine in Litigation Act of 2009: Hearing Before the H.*

Subcomm. on Commercial and Admin. Law, 111th Cong. 24-37 (2009) (statement of Leslie A. Bailey of Public Justice) (hereinafter "Bailey Statement").

[17] FJC Report, at 5.

[18] *See e.g.*, Crow I at 107; Richard A. Zitrin, *The Laudable South Carolina Rules Must Be Broadened*, 55 S.C. L. Rev. 883, 887-890 (2004); Bailey Statement, at 25-28.

[19] *See* Brooklyn Savings Bank v. O'Neil, 324 U.S. 697, 704-08 (1945); Stalnaker v. Novar Corp., 293 F. Supp.2d 1260, 1263 (M.D. Ala. 2003).

[20] *See e.g.*, Dees v. Hydrady, Inc., 706 F. Supp.2d 1227, 1242 (M.D. Fla. 2010).

[21] Crow I, at 107.

[22] *See* Hens v. Clientlogic Operating Corp., No. 05-CV-381S, 2010 WL 4340919, at *3 (W.D.N.Y. Nov. 2, 2010).

[23] *See, e.g.*, Taylor v. AFS Tech., Inc., No. CV-09-2567, 2010 WL 2079750, at * 2-3; Poulin v. General Dynamics Shared Res. Inc., No. 3:09-cv-00058, 2010 WL 1257751, at *2-3 (W.D. Vir. Mar. 26, 2010).

[24] *See, e.g.*, *Dees*, 706 F. Supp.2d at 1242, 1246; White v. Bonner, No. 4:10-CV-105-F, 2010 WL 4625770, at *2 (E.D.N.C. Nov. 4, 2010); *Taylor*, 2010 WL 2079750, at *2.

[25] *See, e.g.*, Tabor v. Fox, No. 5:09-CV-338, 2010 WL 2509907, at * 2 (E.D.N.C. June 17, 2010); In re Sepracor Inc. FLSA Litig., MDL No. 2039, 2009 WL 3253947, at *1 (D. Ariz. Oct. 8, 2009).

[26] *See, e.g., Poulin*, 2010 WL 1257751, at *3; Prater v. Commerce Equities Mgmt. Co., No. H-07-2349, 2008 WL 5140045, at *9-10, (S.D. Tex. Dec. 8, 2008).

[27] *See, e.g., id.* at *3-4.

[28] *See, e.g.*, McCaffrey v. Mortgage Sources Corp., No. 08-2660, 2010 WL 4024065, at *1-2 (D. Kan. Oct. 13, 2010); *In re Sepracor Inc. FLSA Litig.*, 2009 WL 3253947, at *9-10.

[29] *See, e.g., McCaffrey*, 2010 WL 4035065, at *2; *In re Sepracor Inc. FLSA Litig.*, 2009 WL 3253947, at *1-2.

[30] *See, e.g., Hens*, 2010 WL 4340919, at *4; *Tabor*, 2010 WL 2509907, at *2; *Taylor*, 2010 WL 2079750, at *3; *Poulin*, 2010 WL 1257751, at *3; *In re Sepracor Inc. FLSA Litig.*, 2009 WL 3253947, at *3.

[31] *See, e.g., Poulin*, 2010 WL 1257751, at *3; *Prater*, 2008 WL 5140045, at *9; Arthur Miller, *Private Lives or Public Access?*, 77 A.B.A.J. 65, 68 (1991).

[32] *See, e.g., Hens*, 2010 WL 4340919, at *3-4; *McCaffrey*, 2010 WL 4024065, at *2; *Taylor*, 2010 WL 2079750, at *3; *Poulin*, 2010 WL 1257751, at *3; *In re Sepracor Inc. FLSA Litig.*, 2009 WL 3253947, at *2; *Prater*, 2008 WL 5140045, at *9-10.

[33] 276 Va. 375 (2008).

[34] VA. CODE § 8.01-55.

[35] *Perreault*, 276 Va. at 381.

[36] *Id.* at 381-83.

[37] *Id.* at 389-90.

[38] *Id.* at 390. The court also rejected the parties' arguments (1) that if the settlements were unsealed they would not obtain the benefit of their bargain; (2) that their privacy interests were superior to the public's interest in accessing court records; and (3) that the defendant could become a target of nuisance suits. *Id.* at 390-91.

[39] 960 A.2d 405, 407 (N.J. Super. Ct. App. Div. 2008).

[40] *Id.*

[41] *See* Public Citizen Homepage, http://www.citizen.org (2010).

[42] *Verni*, 960 A.2d at 408.

[43] *Id.*

[44] *Id.* at 409-11.

[45] 142 N.J. 356 (1995).

[46] *Id.* at 371-83.

[47] *See also* Gleba v. Daimler Chrysler Corp., 13 Mass. L. Rptr. 576, 2001 WL 1029678 (Super. Ct. Mass. 2001) (rejecting a motion to seal a settlement agreement and applying Massachusetts law regarding sealed discovery to a sealed settlement agreement).

[48] 603 F. Supp.2d 673 (S.D.N.Y. 2009).

[49] *Id.* at 674.

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Id.* at 675-76.
[54] *Id.* at 676.
[55] *Compare In re* Sept. 11th Litig., 723 F. Supp.2d 526 (S.D.N.Y. 2010) *with Perreault*, 276 Va. at 383-84 (where the Virginia Supreme Court noted that the court below kept settlement agreements under seal pending appeal).
[56] No. 21 MC 101, 2010 WL 637789, at *1 (S.D.N.Y. Feb. 19, 2010).
[57] *Id.*
[58] *Id.*
[59] *Id.* at *2.
[60] *In re* Sept. 11th Litig., 723 F. Supp.2d 526 (S.D.N.Y. July 1, 2010).
[61] *Id.* at 531.
[62] *Id.* at 531-32.
[63] *Id.* at 532.
[64] *Id.*
[65] *Id.* at 533.
[66] *See In re* Sept. 11th Litig., 723 F. Supp.2d 534 (S.D.N.Y. 2010).

New Developments in PRC Privacy Laws following the First "Cyber Manhunt" Cases

By Ariel Ye and David Gu

THE "Cyber Manhunt" engine is an Internet engine which utilizes participation by Internet users to filter search results and assists users in clarifying their search requests. Different from the automated search results from Google and Chinese Baidu engines, the cyber manhunt engine mobilizes Internet users to search for and reveal specific useful information about individuals on the Web. Despite its efficiency in identifying useful information, many people find this kind of searching unacceptable because it violates individuals' privacy.

Since 2006, the cyber manhunt has become a popular method for Internet users to "hunt down" those whose actions or comments go against social norms or moral and ethical standards in the PRC. The following three examples may shed some light on how the "cyber manhunt" engine works.

The Abused Cat Incident

In February 2006, an Internet user with the cyber name of "stepping upon broken glass" published some video files on the Internet showing a woman crushing a cat under her high-heel shoes. Soon after, an Internet user named "12ookie-hz" published a link to the videos on the webpage "Mao Pu."[1] Another Internet user "dark consul" uploaded the woman's image to the webpage "Tian Ya"[2], and made a universal "order for arrest" which openly asked all Internet users to find the woman. In order to catch the woman, many Internet users voluntarily donated MPs or even cash in exchange for useful information about her. The reward was increased from 1,000 to 5,000 MPs. In March 2006, an Internet user "I am not an angel in sands" commented on Mao Pu that "this woman is from a small town in Hei Long Jiang Province…." which turned out to be an important clue to other Internet users. About six days after the video clips were published, the identities of three potential "suspects" were made known on the Mao Pu website.

Ariel Ye and David Gu are lawyers at the Beijing office of King & Wood.

The South China Tiger Incident

In October 2007, Mr. Zhou Zhenglong, a peasant in Shan Xi Province, announced that he had taken some pictures of a South China tiger which had been believed for a long time to be an extinct species. In December 2007, the Forestry Department of Shan Xi Province held a news conference to show the pictures to the public and gave Mr. Zhou a reward of around RMB 20,000 for the discovery. Several hours later, some posts were logged on the Internet which questioned the authenticity of the tiger photos. Afterwards, Internet users cast further doubt upon the photos from the perspective of light, shooting angle and their similarity to some drawings in general circulation. On 15 November 2007, an Internet user asserted that the so-

called "tiger photos" looked very similar to some drawings he had in his house. Another Internet user who played an important role in the "abused cat incident" discovered that a traditional Chinese character of "dragon" appeared at the bottom of the photos. As these photos were identified as fakes, Mr. Zhou, the photographer, was arrested, charged and convicted under Article 266 of the PRC Criminal Law of obtaining public money by fraud and sentenced to two years in jail.

The Corrupt Official Incident

In December 2008, Mr. Zhou Jiugeng, the head of Nanjing Jiang Ning District Real Estate Department was tracked by Internet users using the "cyber manhunt" engine. Some photos of Mr. Zhou were published on the Internet, which showed that he wore a very expensive wrist watch, smoked high-priced cigarettes and owned a famous marque of car. Later, Internet users reported that Mr. Zhou's brother was a local real estate developer and that the two were entangled in some corrupt activities together. Since this incident drew significant public attention, the local government was forced to conduct an investigation, which culminated in the arrest of Mr. Zhou on 9 February, 2009.

There are two sides to the "cyber manhunt" coin. On one side, hundreds of thousands of Internet users deem themselves as "Robin Hood on the Internet", acting for justice. As the above examples indicate, through effective interaction on the Internet, they deploy the power of each individual to identify morally uncomfortable and/or illegal incidents, help the authorities to collect useful information and evidence against offenders, and indeed play a role in monitoring social behavior as well as deterring misbehavior.

On the other side, sometimes when self-righteous Internet users expose a person's name, profession, home address and other personal information to the public in the name of "justice," that person becomes a victim as his or her privacy rights are inevitably damaged, either temporarily or permanently.

It is well-known to the world that the Internet has been a fast growing phenomenon in China. It is one of the most popular media - Chinese Internet users already exceed 400 million. At the same time, PRC privacy laws have developed. This paper will touch upon an interesting topic: how the developing privacy laws in China can adapt and respond to the new cyberspace phenomenon, the "cyber manhunt." In the following chapters, this topic will be addressed from the judicial, legislative and academic perspectives.

The First Case of the "Cyber Manhunt" and its Implications

The first published case of the "cyber manhunt" is actually three. In December 2008, the Beijing Chao Yang District Court[3] rendered three separate first-instance judgments in respect of this landmark case. Some excerpts of the judgments are presented as follows:

Wang Fei v. Zhang Le Yi[4]

The Court finds that Wang Fei is Jiang Yan's (the deceased) husband, as

their marital relationship was registered and recorded on 22 February 2006. In the evening of 29 December 2007, Jiang Yan committed suicide by jumping from her house of the 24th floor.

During her life, Jiang Yan registered a personal blog titled as "A Migrant Bird Flying towards the North," and wrote articles in it. About two months prior to her suicide, she blocked public access to her blog but did not stop writing. In her blog, Jiang Yan wrote diaries that recorded her emotional struggles with her failed marriage and published some photos of her husband and Ms. Dong, who were believed to be having an affair together. In these diaries, her husband's name, working address and other personal information was exposed. Before Jiang Yan's first attempt at suicide, she told an Internet user the pin number for access to her blog and asked him to open her blog after 12 hours. After Jiang Yan committed suicide, this Internet user let Jiang Yan's sister know the pin number, and the latter opened the blog.

Jiang Yan's diaries in her blog were read by an unnamed Internet user and forwarded to the discussion forum of the "Tian Ya" website. Consequently, these diaries were published by Internet users on different websites and triggered extensive discussions among different people, many of whom expressed the view that Wang Fei's affair was one of the main factors which cause[d] Jiang Yan's suicide. Some Internet users initiated a "cyber manhunt" on the "Tian Ya" seeking to disclose Wang Fei's name, working address and home address etc. Some abused and humiliated Wang Fei with their words and some others harassed Wang Fei and his parents at their apartments. As one example, on the wall of their houses were painted words such as "immoral household," "the good wife was forced to die," and "blood for blood" etc. Even until the time of this trial, there are still many articles on the Internet providing comments about the incident.

In addition, Zhang Le Yi, the college classmate of Jiang Yan, registered a non-profit website on 11 January 2008, titled "A Migrant Bird Flying towards the North,"[5] (the "**Website**") the same name as Jiang Yan's blog. On the main webpage, Zhang Le Yi introduced this website as "a place to make tributes and seek justice for Jiang Yan." Zhang Le Yi and Jiang Yan's relatives published a number of articles dedicated to Jiang Yan there. Additionally, Zhang Le Yi set up website links to "Tian Ya," "Sina" and so on.

In particular, Wang Fei believed that several articles published on the Website disclosed some details of his affair, his name, working address and home address etc, included defamatory remarks, and therefore violated his privacy right and reputation right.

The legal issue in this case lies in whether Zhang Le Yi's conduct, such as disclosing Wang Fei's real name, working address, home address and his affair on the website he created constitutes an infringement of Wang Fei's privacy right and reputation right.

A. Zhang Le Yi's conduct has infringed Wang Fei's privacy right and reputation right

Privacy generally refers to private life, private information, private space and peace of individual life, which are

deemed as interests attached to specific persons or personhood and which such persons do not wish to disclose to the general public. Privacy right generally means a type of personhood right, by which a natural person is entitled to control his or her private secrets and private life and exclude any interference from the outside. Any conduct such as disclosing or publicizing a person's private information, intruding on this person's private domain or interfering with such person's private activities may constitute a violation of the privacy right belonging to this person.

A citizen's private affair of love, including an out-of-marriage affair, falls squarely within the privacy domain. In a normal social life, such information is only known to a small number of persons and would not be disseminated to a large number of unidentified persons. In the instant case, Zhang Le Yi knew the fact that Wang Fei was involved in an affair, given he was the classmate of Jiang Yan. After Jiang Yan's death, Zhang Le Yi not only publicized this fact on the website he created, but also built website links to other websites, so that this fact was disseminated very broadly on the Internet to those unidentified persons in the public. As such, Wang Fei's privacy right has been infringed.

In addition, in the course of social interaction, a citizen may disclose his or her name, working address, home address and other personal information to others, and such information may be known and utilized in one way or another. Whether the disclosure or use of such information infringes a person's privacy right depends upon the totality of the circumstances, where the manner of obtaining and disclosing such information, as well as the extent of disclosure, the purpose of disclosure and consequences of such disclosure should all be taken into account.

In the instant case, Zhang Le Yi criticized Wang Fei's disloyalty in his marriage with Jiang Yan. Prior to his disclosure of Mr. Wang's affair and personal information, Zhang Le Yi had actual knowledge that such information when disclosed by him would be received by unidentified persons, and could foresee any relevant consequences arising from this disclosure. Therefore, Mr. Zhang's intent could be inferred from his conduct including disclosing Wang Fei's affair and his personal information. After such information was disclosed, Wang Fei's identity became known to Internet users in the public, and many provocative comments were made against him as a result. When Zhang Le Yi criticized Wang Fei's disloyalty to his wife, he should not have disclosed Wang Fei's actual name, working address and home address etc. Because he did, Wang Fei's privacy was violated.

Reputation refers to an objective and comprehensive societal judgment upon a specific civil person's[6] characteristics, skills and other features. Reputation right means a type of personhood right to maintain society's judgment and one's own judgment of one's intrinsic features and values as a civil person.

The private information disclosed about Wang Fei not only triggered endless criticisms and public outrage from Internet users, but also caused them to adopt the "cyber manhunt" engine to search for other information in relation to Wang Fei and his parents. Later, this

search resulted in intensive and continuous personal attacks towards Wang Fei on the Internet, and some harassment to Wang Fei's peace of life. In this regard, the societal judgment of Wang Fei has been severely downgraded, directly because of Zhang Le Yi's misbehavior. Thus, Zhang Le Yi has infringed Wang Fei's reputation right by disclosing his private information in public.

B. Zhang Le Yi's Liability for His Malfeasance

Zhang Le Yi, as the registered administrator of the Website, has a right of free speech to write articles on his own and publish articles written by others on the Website. However, the exercise of his right should be consistent with applicable laws and regulations, and in particular it should not infringe the legitimate interests of others. However, this was not the case here.

Accordingly, this Court holds that: (a) three articles published on the Website should be deleted and a public apology should be made from Zhang Le Yi to Wang Fei on the Website; (b) the request for loss of salaries and wages is not sustained; (c) the request of public notary payments of RMB684 is sustained; (d) damages for mental suffering is sustained, but the amount should be reduced to RMB 5,000 considering: (i) prior to the information being disclosed, Jiang Yan's blog had been open to the public, such that Zhang Le Yi's disclosure of private information was only one reason, not the sole reason which caused Wang Fei's anguish; (ii) when administering the Website, Zhang Le Yi did voluntarily delete some infringing information; (iii) Other than Zhang Le Yi's conduct, there were other things which caused the information to be disclosed, such as Jiang Yan's blog and the "cyber manhunt" engine adopted by Internet users on other websites; and (iv) Wang Fei's disloyalty to his wife is a fact and should be criticized in terms of the social norms.'

Wang Fei v. Beijing Ling Yun Interactive Information Technologies Co., Ltd.[7]

The website of "www.daqi.com" ("**Daqi**") is a for-profit website registered and administered by Ling Yun Interactive Information Technologies Co., Ltd. ("**Ling Yun Company**"). As Jiang Yan's suicide drew the attention of the public, a special webpage was created on Daqi, titled "the last blog diary from the woman who committed suicide by jumping from the 24th floor" on 14 January 2008. The webpage mainly included: an introduction about Jiang Yan's suicide; relevant web-post links; a site report about Internet users' voluntary tributes at the place where Jiang Yan's suicide took place; a site report about Internet users; phone interview records with Jiang Hong (Jiang Yan's sister), Zhang Le Yi (Jiang Yan's classmate) and the lawyer who represented Jiang's family; Internet users' messages; and "psychological analysis" etc. On the webpage, the real names of Wang Fei, Jiang Yan and Ms. Dong were adopted, and some photos of Jiang Yan, Wang Fei and Ms. Dong, Internet users' tributes on the site and the defacement of Wang Fei's apartment were published as well. Under the photo of Wang Fei and

Ms. Dong, a number of words read as "the photo with the third-party during the Rome visit organized by Wang Fei's company."

It seems proper for Daqi to set up a special webpage analyzing the incident, since it has the freedom to disseminate news in the public domain. That said, where Daqi exercised this right, it should have taken any technical measures of redacting private information and photos, so as not to infringe others' privacy right and reputation right.'

Wang Fei v. Hainan Tian Ya Online Website Technologies Co., Ltd[8]

The website of "www.tianya.cn" ("**Tian Ya**") is a for-profit website registered in March 1993. Its users number approximately 20 million. This website provides rules such as "The fundamental laws of Tian Ya" and "The censorship measures of key words" etc. In terms of these regulations, there are four layers of monitoring in respect of monitoring posts submitted by Internet users, including most sensitive key words monitoring, very sensitive key words monitoring, relatively sensitive key words monitoring and sensitive key words monitoring.

On 15 March 2008 (prior to the filing of the case), Tian Ya deleted relevant articles and comments regarding the incident from its website.

The administrator of Tian Ya should be responsible for monitoring any articles and posts published on its website. Since Tian Ya has set forth relevant rules regarding monitoring and censorship measures, it has fulfilled its duty as the administrator. On the other hand, Chinese characters are rich and diverse, and may be combined in various expressions of cyberspace language. Under the circumstances, it would be very difficult for websites to monitor every word. So far, even if the latest website management and technological measures are adopted, the website administrator may not perform censorship of every post in advance. As such, the monitoring duty owed by the website is conditioned on the basis that it cannot always know whether published articles or comments are illegal or tortious in nature or infringe others' lawful interests. Where such knowledge exists, and the website disregards existing unlawful articles and comments, and allows their dissemination, then the website breaches its duty and indeed infringes others' rights; if it timely deletes such articles or comments, then its duty are fulfilled.

In the instant case, Tian Ya's duty of monitoring may be fulfilled as long as it has deleted or modified infringing information since it was aware of such information on its website or had actual knowledge of it after the infringed's complaint. In fact, Tian Ya did delete the articles and comments prior to the filing of the case. Therefore, this Court holds that Wang Fei's allegation that Tian Ya infringed his privacy right and reputation right has not been established.'

The "Cyber Manhunt" Case's Implications

Several progressive steps in relation to PRC privacy laws have been made in the above case. First, the Court did not arbitrarily hold that the "cyber manhunt" was illegal *per se*, since not every so-

called "cyber manhunt" will unavoidably intrude individuals' privacy. Indeed, the Court did not address the issue of the "cyber manhunt" extensively. Instead, the Court took an indirect approach to deal with the "cyber manhunt," and offered an opinion that websites should at least be responsible for posts or comments published by their users on their webpages.

In particular, the Court provided a set of rules for finding liability in response to different behaviors on the Internet. In the case involving Zhang Le Yi, the Court reasoned that the administrator of a personal website should be responsible for articles or comments made by himself on his personal website. If such articles or comments are found to be tortious in nature (e.g. they disclose a person's private information or violate a person's right of reputation), some liability would be imposed upon the administrator.

In addition, a similar rule was adopted in the case involving Daqi. This website functions by collecting some published articles or comments from other websites and then creating a dedicated webpage where a hotly-debated subject is raised for further discussion. The Court's rationale was that the website should take responsibility for monitoring any published articles or comments in it, regardless of whether they were originally made or reprinted from other sources. The Court further opined that the collected information, even if it was not original but reprinted, may still constitute a source of infringement of a privacy right, due to its implicitly tortious nature. Nevertheless, the Court distinguished reports on Daqi's site from Zhang Le Yi's personal posts, and held that Daqi's reports were news reports. Therefore, the Court held that Daqi must live with the rules and disciplines that apply to traditional media, and should have "redacted private information and photos using technical measures". If it did not, its liability for infringement of the right of privacy would be established.

Finally, the Court provided some guidelines for websites like Tian Ya, "where the website administrator has actual knowledge of illegal or tortious information which is detrimental to others' lawful interests, but disregards its existence or dissemination, it should be liable for its infringement of such rights; however, if the administrator deletes this information in a timely manner, then it would be safe from any liability." This rule is similar to the "safe haven" rule in IP cases, and some commentators believe it is innovative, though it may not be well-drafted.[9] In any event it is very encouraging and impressive to see the Chinese Court craft different rules to accommodate nuances between traditional media like Daqi (a news website) and newly-developed media like Tian Ya and personal blogs.

Furthermore, this case is prominent because for the first time Chinese judges have tried to define privacy and the privacy right in their own terms, and to independently address significant issues in relation to privacy law, rather than having calibrated them to adhere to the traditional scheme of reputation right infringement. The effects that this case brings about in PRC privacy law will be further addressed in the remainder of this paper.

The Legislative Efforts for Developing the PRC Privacy Laws

The landscape of Chinese privacy law has significantly changed since the 1980s. On 12 April 1986, the General Provisions of the Civil Law of PRC (the "**Civil Law**") was promulgated by the National People's Congress (the "**NPC**"). Under the Civil Law, the chapter on "personhood rights" is independent from the chapter on "civil entities." The separation of the two chapters reflects the fact that "personhood rights" were not deemed as an ancillary to "civil entities" any more, but a totally different subject matter of civil law rights. Under the chapter of "personhood rights," several rights are enumerated, among them name right, image right, and reputation right. Nonetheless, privacy right is not included among these, and neither were specific privacy laws legislated at that time.

In addition to the Civil Law, numerous judicial interpretations made by the Supreme Court of China[10] have enriched the body of Chinese privacy law. In the Several Opinions of Implementation of the Civil Law dated on 2 April 1988, Article 140 states that, "disclosing a person's privacy to the public, in writing or orally, or fabricating facts to publicly humiliate a person, as well as insulting or defaming a person's reputation with some consequences arising therefrom, shall constitute a violation of a citizen's reputation right." In this interpretation, the concept of "privacy" was adopted for the first time,[11] though its substance under this law may not be as rich as in some western privacy laws. Nevertheless, the inclusive term of "privacy" in this legal context became a starting point for further developments of PRC privacy laws. Under this legal scheme, however, it bears emphasis that any violation of privacy is deemed a violation of reputation right and there is no independent legal remedy provided for privacy right infringement.

Afterwards, the substance of the privacy right was further expanded by other judicial interpretations. In the Answers for Several Questions regarding Trials of Reputation Right,[12] Article 7 (3) added some key words such as "without a person's consent" or "unilaterally publicizing or disclosing private information" to define the concept of privacy. These newly-added terms demonstrate one crucial element of privacy infringement --- it is against the will of a person who is entitled to freely dealing with his or her privacy. In the same interpretation, Article 8 provides that information regarding sexually-transmitted diseases can be deemed as private information deserving of protection. In this regard, the substance of privacy expands from the interpersonal relationship area to medical and health. In the Explanations of Several Questions as to Calculating Liabilities and Damages for Mental Sufferings arising from Civil Infringements dated 10 March 2001, the Chinese Supreme Court took the position that privacy interests could be directly protected by civil proceedings, rather than indirectly by claiming remedies for violation of a reputation right.[13] In other words, any violation of privacy interests becomes actionable, [14]even if a privacy right has not been recognized as a separate type of personhood right under this interpretation.

Recently, the most important milestone legislation relates to promulgation of the Law of Tortious Liability of the People's Republic of China dated 26 December 2009. Under Article 2 of this law, "privacy right" is expressly recognized as one of the enumerated civil law rights, together with name right, image right, reputation right, parenting right, intellectual property right and shareholder right.[15] From this time on, "privacy right" becomes a right, more than a bundle of interests related to the reputation right.

It is well-known that China's legal system is rooted in civil law traditions and its lower court judges do not make laws, but follow the NPC's legislation and the Chinese Supreme Court's judicial interpretations (which are quasi-legislative in nature). In the first case of "cyber manhunt," the judges not only defined in detail privacy and the privacy right, but also extended the legal analysis of privacy law from the traditional arena (e.g. interpersonal relationships) to those in the cyberspace, where both the NPC and the Chinese Supreme Court have not done so. Slightly deviating from the conservative tradition that a civil law judge must follow laws, the judges in this case may have liberally broadened the substance of privacy or the privacy right, to the extent that includes rights for private space or peace of individual life, concepts which have been cited and discussed by Chinese legal scholars for a period of time. Nevertheless, it is not the first time for Chinese courts to provide judicial guidelines for the public, even if these rules are not precedents.[16]

After the triple judgments were rendered, only Zhang Lei Yi appealed. The appellate court held that Mr. Zhang should be liable for his violation of Wang Fei's reputation right by exposing Mr. Wang's privacy to the public, and affirmed most parts of the first-instance judgments, except slightly reducing the damages awarded. Apparently, the appellate court took a conservative approach and judged the case within the boundaries of existing laws and judicial interpretations, rather than making new laws or creating fresh ideas beyond these existing limits.

Academic Contributions and Criticisms

Compared to conservative judges, Chinese legal scholars are more liberal and free to introduce new ideas and constructive thoughts with regard to privacy laws, particularly where existing laws are less mature with some gaps to fill in. Additionally, academic criticism has contributed some meaningful developments to this subject.

From an academic perspective, because the body of PRC privacy laws is currently growing, it appears that the trend of expanding privacy rights will not stop in the future. However, the extension of protection of privacy rights is not unfettered. Some commentators believe a foreseeable limitation upon privacy right relates to the "cyber manhunt" phenomenon, where the conflict between privacy right (the claimed right by Wang Fei) and right to learn the truth (the right possibly claimed by Internet users who conduct the "cyber manhunt") and the boundary between each right will become a hotly debated topic.[17] Another interesting topic relates to how much privacy a public figure could enjoy. A football star, a famous singer or a

politician could be viewed by the public as someone whose privacy should be protected in a limited way, in contrast with ordinary people.[18] Therefore, publicity law is another related area where scholars will delve.

Some commentators believe that a "privacy right" is unambiguously recognized and included in the Tortious Liability Law, but conclude that this law fails to articulate how liability should be established. According to this law, it is suggested that a general tort liability rule should come into play, where four elements must be presented, in order to establish any liability for infringement of privacy: (a) illegal conduct; (b) damages; (c) causation: (d) scienter that refers to either intentional infringement or negligent infringement.[19] The infringed bears the burden of proving these elements to establish a valid case.

In order to resist or limit such liability, the defendant may raise certain defenses, such as the infringed's consent, limited privacy for public figures or right to learn the truth. Damages for mental suffering is one of the remedies which the infringed may seek. But the threshold to trigger this remedy is that mental suffering should be severe. As suggested, "severe" mental suffering may be found, so long as a reasonable person would believe that such suffering caused by the infringement is generally intolerable and unacceptable.[20] Accordingly, "severe" should not be interpreted too strictly by courts.[21]

Finally, the current academic movement is to suggest that a prospective Civil Code of the PRC contain a chapter on "personhood rights", in which privacy right should be expressly defined, and the elements of establishing privacy infringement should be laid down in clear and straightforward language.[22]

Conclusion

In conclusion, the triple judgment in the landmark cases relating to the "cyber manhunt" of Wang Fei demonstrates that the Chinese privacy right has been expanded from the traditional arena of interpersonal relationships to cyberspace, and PRC privacy laws have developed in depth and breadth, due to tremendous efforts made by Chinese legislators, courts and scholars.

There is an evident trend that this privacy right will continue to be clarified. Chinese legislators and courts may continue to take a relatively conservative approach to putting any legal developments in this area within the framework of existing law. However, legal scholars are evidently willing to take the lead and to accelerate discussion of legal reform of privacy laws in China.

---

[1] The "cyber manhunt" phenomenon originally started from this website. Like many other worldwide studying forums, people ask questions on the "Mao Pu" site, and are willing to pay for answers using a type of Internet currency called MP. Those who provide answers in exchange for MP are called "reward hunters". The most MPs go to those reward hunters who can quickly respond to questions with accurate and comprehensive answers.

[2] This is one of a number of popular websites where the "cyber manhunt" engine is used.

[3] The Chao Yang District Court is the first-instance court and has jurisdiction on these cases.

[4] Chao Min Chu Zi No. 10930 (2008).

[5] This website address is http: orionchris.cn.

[6] Civil person may refer to a natural person, legal person, and other non-legal-person organization.

[7] Chao Min Chu Zi No. 29276 (2008).

[8] Chao Min Chu Zi No. 29277 (2008).

[9] "The Analysis of the three first-instance judgments of the first case of "cyber manhunt'," page 66, Hu Lin, <Legal Application>, issue 7 (2009).

[10] In relation to fundamental laws such as the Civil Law, the Chinese Supreme Court has quasi-legislative power to provide interpretations of laws. These judicial interpretations are part of China's binding written law.

[11] The term of "privacy" appears in several laws, including article 30 of <Juvenile Protection Law of PRC> dated 4 September 1991, Article 39 of <Women Rights Protection Law of PRC> dated 3 April 1992, and Article 30 of <the Fundamental Laws of Macau SAR of PRC> dated 31 March 1993.

[12] This judicial interpretation was promulgated to the public on 7 August 1993. Article 7 (3) provides, " without a person's consent, unilaterally publicizing this person's private materials or disclosing his privacy in writing or orally, to cause damages to such person's reputation, may constitute violation of this person's reputation right."

[13] Article 1 provides, "… when privacy or any other types of personhood interests are violated, the infringed may file lawsuit in Chinese courts, seeking for damages of mental sufferings, given the cause that such interests are infringed, and Chinese courts shall accept this filing."

[14] According to the Regulations of Cause of Action in Civil Lawsuits dated 4 February 2008, the "privacy right dispute" is listed, among others, as a separate cause of action.

[15] However, the term of "privacy right" was first adopted in another legal context, i.e. in the Women Rights Protection Law of the PRC (Modified in 2005).

[16] A county court in Si Chuan held that "the parent-child relationship" does not fall within the category of privacy (2000); another district court in Shanghai held that "a citizen's name, home address, personal hobbies as her private information as well as peace of her life should be protected by laws and should not be publicized, utilized and infringed" (2000).

[17] "The New Developments of Privacy Right", this speech note was given by Professor Wang Liming, at the forum of Legislative Research of Tortious Liability Law of PRC. This note can be found at http://www.civillaw.com.cn/ggf/weizhang.asp?id=45431, browsed on 14 November 2010.

[18] "The Developments of PRC Privacy Laws", Zhang Xinbao, <National Procurator Academics Journal>, volume 18 no. 2 (April 2010).

[19] "The Establishment of Infringement of Privacy and Its Stereotype Research>, Ma Te, <Young Scholars Forum>, 2007.

[20] "The Developments of PRC Privacy Laws", Zhang Xinbao, <National Procurator Academics Journal>, volume 18 no. 2 (April 2010).

[21] *Id.*

[22] "The New Developments of Privacy Right", Professor Wang Liming, <The People's University Law Review>, (2009); "The Three Most Important Questions to be Solved for Legislating the Personhood Laws of PRC", Professor Yang Lixin, <National Procurator Academics Journal>, volume 16 no. 3 (June 2008).

Crispin v. Christian Audigier, Inc.: The Struggle to Maintain Privacy In The Face Of New Forms of Electronic Communication

By Nichole Cohen, M. King Hill, III and Craig A. Thompson

COURTS have traditionally struggled to keep pace with the rapidly changing fields of science and technology. One area of particular and constant struggle is that of information technology. Access to electronically stored information is an issue in nearly all complex civil litigation today. Balancing a litigant's right to discover electronic information with individual privacy concerns is a particularly difficult task for the courts. This article explores what is being touted as the newest and perhaps most revolutionary form of electronic communication – Facebook Messages – and how the courts might balance a party's entitlement to litigation discovery with individual privacy concerns in light of this new way of communicating.

M. King Hill, III is a partner with Venable LLP in the firm's Towson, Maryland office. His practice focuses on products liability and personal injurt litigation.

Craig A. Thompson is a partner who practices in the same areas in Venable's Baltimore office.

Nichole Cohen is an associate who works closely with the same practice group in the firm's Baltimore office.

I. What is "Facebook Messages?"

Facebook, the world's most visited website,[1] announced in November that it will unveil what CEO Mark Zuckerberg believes is the future of modern communication: Facebook Messages.[2] The new messaging system's three anticipated "features" are seamless messaging, conversation history, and a "social inbox."

II. Seamless Messaging

The new messaging system will combine multiple forms of communication – including text messages, e-mail, online chats and instant messages, and traditional Facebook messages – into one unified "social inbox."[3] According to Facebook engineers, Facebook Messages is designed to allow users to exchange messages without regard to the form of communication.[4] Users can send and receive SMS messages (*i.e.*, text messages), e-mails, chats, and traditional private messages from one centralized location.[5] In Facebook's words, you simply choose a person and type a message;[6] the medium of communication is immaterial.

In addition to sending messages, chats or instant messages, and SMS (text), Facebook Messages will also allow users to send and receive e-mails. While Facebook's new messaging framework is not e-mail,[7] Facebook Messages provides every Facebook user with an @Facebook.com e-mail address. Individuals without Facebook accounts

can communicate with Facebook users via a user's @Facebook.com e-mail address. In other words, you can now use Facebook to communicate with your friends and colleagues who do not have Facebook accounts by giving them your @Facebook.com e-mail address. It remains to be seen whether Facebook will allow users to send messages from other e-mail services like Hotmail or Gmail.

Like traditional e-mail, Facebook Messages will allow users to forward e-mails and send attachments (not only links and photographs, but also external files).[8] Yet unlike traditional e-mail, e-mails sent and received through Facebook will not have traditional cc, bcc or subject lines because, according to Zuckerburg, those are formalities that are unneeded, and even unwanted, in a modern messaging system.[9] By adding some features normally found in e-mail and removing others, Facebook Messages is designed to resemble text messaging, with the hope that users will find it to be "informal, immediate, personal, simple, minimal, and short."[10]

III. Conversation History

Facebook lauds its new Facebook Messages feature as archiving and organizing all of a user's conversations -- no matter the medium -- in one location.[11] By threading messages, Facebook Messages provides users with a single history of every conversation with a particular person. For example, if you communicate with your college friend Dan using SMS (text) messages, e-mail, and traditional Facebook messages, Facebook Messages will thread all of your messages sent to and received from Dan since the beginning of your Facebook-based communications together in one location. In Facebook's words: "You can see everything you've discussed with each friend as a single conversation."[12]

IV. Social Inbox

In addition to providing Facebook users with a means to communicate with individuals outside Facebook, Facebook Messages will also condense all of a user's correspondence – of all types – into one prioritized Social Inbox.[13] Unlike traditional e-mail, using an @Facebook.com e-mail address allows users (by default) to receive only messages from their Facebook friends and friends of friends. Rather than having e-mails from friends and family appear sandwiched between bills and junk mail, Facebook Messages provides its users with a list of messages organized by sender. Of course, @Facebook.com users will still receive unsolicited e-mails, but they will be segregated into an "Other" folder, much like a more conventional "Spam" folder.

V. Facebook's Reach

To be sure, Facebook-based communication is widespread: Facebook has over 500 million users, 350 million of which send over 15 billion "person-to-person messages" each month using Facebook's current messaging infrastructure, and Facebook's instant message service enables over 300 million users to send more than 120 billion messages each month.[14] Facebook Messages --not to be confused with the

existing message infrastructure now in use -- is currently being offered by invitation only, and Facebook plans to roll out Facebook Messages to all users in the coming months.[15]

VI. Facebook and the Stored Communications Act[16]

Private messages exchanged on social networking sites are now protected from disclosure by social networking providers served with non-party civil subpoenas, at least according to one court. In May 2010, the U.S. District Court for the Central District of California issued an order quashing subpoenas served on Facebook and MySpace, Inc. ("MySpace") and website hosting company Media Temple, Inc. ("Media Temple") because these businesses qualified as electronic communication service (ECS) providers and remote computing service (RCS) providers under the Stored Communications Act (SCA).[17]

VII. About the SCA

The SCA prohibits RCS providers and ECS providers -- with some exceptions[18] -- from knowingly disclosing (either voluntarily, or involuntarily in response to direction from the government) an individual's private communications or records.[19] ECS providers are "any service which provides to users thereof the ability to send and receive wire or electronic communications," and RCS providers supply "to the public computer storage or processing services by means of an electronic communications system,"[20] which includes "any wire, radio, electromagnetic, photooptical or photoelectronic communications and any computer facilities or related electronic equipment for the electronic storage of such communications."[21] A person or entity who does not qualify as an RCS or ECS provider can "disclose with impunity the contents of an electronic communication unlawfully obtained from electronic storage."[22]

VIII. *Crispin v. Christian Audigier, Inc.*

Crispin v. Christian Audigier, Inc. involved copyright infringement and breach of contract claims by artist Buckley Crispin against Christian Audigier, his clothing company, and its sublicensees alleging that Audigier violated an oral license granting Audigier the right to use specific works of Crispin's art in the manufacturing of certain types of clothing.[23] In connection with the suit, the defendants served document subpoenas on four non-party businesses, including Facebook, MySpace, and Media Temple. The subpoenas sought Crispin's subscriber information, all communications between Crispin and a particular artist, and all communications referring or relating to Audigier, his clothing company, the Ed Hardy brand (which was also designed by Audigier), and any of the defendant sublicensees.[24] The defendants claimed that the information sought in the subpoena was relevant to the nature of the alleged oral license between Crispin and Audigier.[25]

Crispin filed a motion to quash the subpoenas on three grounds, including that the subpoenas sought electronically

stored information protected from disclosure under the SCA.[26] Magistrate Judge John E. McDermott held that the SCA did not apply to Facebook, MySpace, or Media Temple, that the SCA does not protect ECS providers from disclosure compelled by subpoena, that the SCA only prohibits ECS providers from disclosing communications held in "electronic storage," and that the communications in question were not held in "electronic storage" as defined by the SCA.[27]

IX. Facebook, MySpace, and Media Temple's Status as "Providers"

On reconsideration, District Judge Margaret M. Morrow found that the communications in question were protected from disclosure because Facebook, MySpace, and Media Temple qualified as both ECS providers and RCS providers under the SCA. Citing (among other decisions) the Ninth Circuit's decisions in *Quon v. Arch Wireless Operating Co.*[28] and *Thoefel v. Farey-Jones*,[29] Judge Marrow found that the providers of text messaging and e-mail services qualified as ECS providers because they enabled users to send and receive electronic communications.[30] After recognizing that Facebook, MySpace, and Media Temple provide "private messaging or e-mail services" like traditional web-based e-mail providers, Judge Morrow held that all three sites were ECS providers within the meaning of the SCA.[31]

A. Are the private messages and e-mails in "electronic storage?"

Determining that the sites qualified as ECS providers was only the first step in the *Crispin* court's analysis because ECS providers are only prohibited from divulging "the contents of a communication while in electronic storage by that service."[32] Under the SCA, the term "electronic storage" refers to "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[33] Evaluating whether an ECS provider holds a communication in electronic storage also implicates the statute's provisions regarding RCS providers. An RCS provider:

> may not divulge the content of any communication received by electronic transmission that is carried or maintained on its service for a customer or subscriber "solely for the purpose of providing storage or computer processing services to [the] subscriber or customer, if the provider is not authorized to access the contents of [the] communications for purposes of providing ... services other than storage or computer processing."[34]

After analyzing decisions from various circuits, the *Crispin* court held that, with respect to messages (*i.e.*, Facebook and MySpace private messages

and Media Temple's e-mail messages) that had not been opened and/or read by the recipient, the three sites operated as ECS providers and the relevant messages were held in "electronic storage" because such storage was "temporary" and "immediate" under the SCA. With respect to messages that had been read and retained by the addressee, the three sites operated as RCS providers supplying storage services under the SCA.[35]

B. Are Facebook wall posts and MySpace comments in "electronic storage?"

The *Crispin* defendants' subpoenas also sought production of Crispin's Facebook wall and MySpace postings.[36] In evaluating whether these postings were protected, Judge Morrow compared them to an electronic version of the traditional "cork-and-pin bulletin board," and noted that the level of privacy a user selects when determining who can view these communications is important: "Unquestionably, the case law… require[s] that the [bulletin board service ("BBS")] be restricted in some fashion; a completely public BBS does not merit protection under the SCA."[37] A private BBS, on the other hand, fits within the SCA's definition of ECS and is protected from disclosure based on SCA legislative history and court precedent.[38] So long as access to the Facebook wall posts and MySpace comments is restricted in some way, the court held that the sites are ECS providers.[39]

While e-mail communications held in electronic storage by an ECS provider are protected under the SCA, Facebook wall posts and MySpace comments present a more difficult question because "in the context of a social-networking site such as Facebook or MySpace, there is no temporary, intermediate step for wall postings or comments…there is no step whereby a Facebook wall posting must be opened, at which point it is deemed received."[40] This complexity led the *Crispin* court to a somewhat incongruous result. Noting precedent standing for "the proposition that a user's or an ECS provider's passive decision not to delete a communication after it has been read by the user renders that communication stored for backup purposes as defined in the statute," the court held that "a Facebook wall posting or a MySpace comment is not protectable as a form of temporary, intermediate storage."[41] In other words, since there is no period when a Facebook wall post or MySpace comment is being held in storage before it is viewed by the recipient, the communications are only protected if held for backup purposes when the user opts not to delete the communication.

Alternatively, Judge Morrow held that Facebook and MySpace also qualified as RCS providers under the SCA. The court analogized Facebook wall posts and MySpace comments to videos posted (and subsequently stored) on YouTube that the user can keep private using YouTube's privacy settings.[42] Facebook wall posts and MySpace comments are similarly "accessible to a limited set of users selected by the poster and are stored on a page provided by the website."[43] However, because the court did not have information regarding Crispin's privacy settings and the extent to which Crispin allowed or denied access to his Facebook

wall and MySpace comments, Judge Morrow remanded the issue for an evidentiary hearing on these questions.[44]

X. *Crispin* and the Future of Electronic Communication Privacy

It remains to be seen how the SCA will apply to Facebook's new and potentially revolutionary messaging system. After all, the SCA was drafted "before the advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994," and "is not built around clear principles that are intended to easily accommodate future changes in technology."[45] "As a result, the existing statutory framework is ill-suited to address modern forms of communication," and "[c]ourts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results."[46]

It seems unlikely that a court following *Crispin*'s analysis would distinguish between e-mail sent through Facebook Messages using an @Facebook.com e-mail address, traditional e-mails, or private person-to-person Facebook Messages. The *Crispin* court protected Crispin's private Facebook messages by analogizing those messages to traditional e-mail, the latter of which has been consistently treated as protected under the SCA. If private Facebook messages and traditional e-mails are both protected from non-party disclosure pursuant to a civil subpoena, it is likely that e-mails sent using Facebook Messages would receive similar protection.

One of the claimed features of Facebook Messages is its cataloging of a user's conversations into one centralized location, or "Conversation History." Facebook analogizes this feature to a shoebox full of love letters beginning with a couple's first meeting, continuing through their courtship, and up to and including a message about which parent is picking up their child from soccer practice.[47] The cataloging of e-mails, SMS messages, chats, and private messages seems to qualify as long-term storage of communications consistent with the services supplied by an RCS provider under the SCA. It appears that the courts have not yet tackled the issue of whether instant messages exchanged through Facebook are protected under the SCA. Does grouping instant messages with e-mails and private messages -- which clearly are protected under the SCA -- automatically insulate instant messages from disclosure pursuant to a civil subpoena served on a non-party? *Crispin* certainly seems to suggest a willingness to extend privacy protections to new forms of electronic communication in the context of non-party civil subpoenas.

XI. Obtaining Otherwise Private Electronic Information by Other Means

The court in *Crispin* was only confronted with the issue of whether the relevant communications were protected under the SCA from compelled disclosure by a non-party civil subpoena. Interestingly, the SCA deals primarily with government demands for disclosure of electronic communications; the SCA

does not explicitly reference the service of civil document subpoenas.[48] Troubled by the notion of "a user's entire portfolio of stored communications and data [becoming] fair game for an adversary," the *Crispin* court created essentially a blanket immunity with respect to civil subpoenas by interpreting "the absence of a provision in the [SCA] for compelled third-party disclosure to be an intentional omission reflecting Congress's desire to protect users' data, in the possession of a third-party provider."[49] Some of the electronic communications protected from disclosure pursuant to a non-party civil subpoena under *Crispin* would still be subject to compelled disclosure to a government entity under certain circumstances as stated in 18 U.S.C. § 2703.[50] Moreover, some, or perhaps all, of the communications protected from non-party discovery under *Crispin* could nonetheless be subject to production in response to discovery requests served on adversarial parties.[51]

The *Crispin* decision represents one court's attempt to reconcile ever-changing information technology with individual privacy rights and a litigant's right to discovery of electronic information. As Facebook continues to embed itself in our communicative lives, it seems inevitable that other courts will have to tackle the daunting task of evolving our jurisprudence to keep pace with, or at least catch up to, information technology innovations like Facebook Messages. Until then, under the *Crispin* analysis, Facebook users should be able to continue to communicate via Facebook and enjoy the protections of the SCA in the context of non-party civil subpoenas.

---

[1] Daniel Ionescu, *Google Names Facebook Most Visited Site*, PC WORLD, May 28, 2010, http://www.pcworld.com/article/197431/google_names_facebook_most_visited_site.html.

[2] Miguel Heft, *Facebook Offers New Messaging Tool*, N.Y. TIMES, Nov. 15, 2010, http://www.nytimes.com/2010/11/16/technology/16facebook.html?_r=1&scp=1&sq=facebook%20messages&st=cse.

[3] Joel Seligstein, *See the Messages that Matter*, THE FACEBOOK BLOG, Nov. 15, 2010, http://blog.facebook.com/blog.php?post=452288242130.

[4] *Id.*

[5] Heft, *supra* note 2.

[6] Seligstein, *supra* note 3.

[7] *Id.*

[8] Help Center, The Facebook, http://www.facebook.com/help/?page=18845 (last visited 12/7/2010)

[9] Gabriel Perna, *Facebook Debuts New Messaging Service*, INTERNATIONAL BUSINESS TIMES, Nov. 16, 2010, http://www.ibtimes.com/articles/82363/20101116/facebook-messaging-e-mail-mark-zuckerberg.htm.

[10] Bianca Bosker, *Facebook Unveils Email Addresses, New Messaging Features*, THE HUFFINGTON POST, Nov. 15, 2010, http://www.huffingtonpost.com/2010/11/15/facebook-email-addresses-_n_783697.html#s182605.

[11] Seligstein, *supra* note 3.

[12] *Id.*

[13] *Id.*

[14] Kannan Muthukkaruppan, *The Underlying Technology of Messages*, Nov. 15, 2010, http://www.facebook.com/notes/facebook-engineering/the-underlying-technology-of-messages/454991608919.

[15] Seligstein, *supra* note 3.

[16] 18 U.S.C. §§ 2701-12.

[17] Crispin v. Christian Audigier, Inc., 717 F. Supp.2d 965 (C.D. Cal. 2010).

[18] ECS and RCS providers ***may*** disclose the contents of a communication to third parties in several instances, including, *inter alia:* (i) to the intended addressee of the communication;

(ii) with consent of the originator or addressee (or subscriber, in the case of RCS providers) of the communication; (iii) to a person employed or authorized or whose facilities are used to forward such communication to its destination (iv) as necessary for the provider to render service, or to protect the right or property of the provider; (v) to law enforcement agencies if the contents "were inadvertently obtained by the service provider, and appear to pertain to the commission of a crime;" (vi) "to a governmental entity if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." 18 U.S.C. § 2702(b)(1), (3), (4), (5), (7), and (8). A government entity can compel ECS and RCS providers to disclose electronic communication -- to varying degrees -- using: (1) a subpoena; (2) a subpoena with notice to the subscriber; (3) a court order issued pursuant to 18 U.S.C. § 2703(d); (4) a court order issued pursuant to § 2703(d) with prior notice to the subscriber; and (5) a search warrant issued according to the requirements of the Federal Rules of Criminal Procedure or state warrant procedures. 18 U.S.C. § 2703. The extent of the compelled disclosure varies depending on the mechanism used by the government entity, and on the classification of the relevant provider as an ECS or RCS provider.

[19] 18 U.S.C. § 2702(a).

[20] 18 U.S.C. § 2711(2).

[21] 18 U.S.C. § 2510(14).

[22] *Crispin*, 717 F. Supp.2d at 973 (quoting Wesley College v. Pitts, 974 F. Supp. 375, 389 (D.Del. 1997) (citing 18 U.S.C. § 2702(a))).

[23] *Crispin*, 717 F. Supp.2d at 968.

[24] *Id.* at 969.

[25] *Crispin*, 717 F. Supp.2d at 969.

[26] *Id.*

[27] *Id.* at 969-70.

[28] 529 F.3d 892 (9th Cir. 2008). According to Judge Morrow, the court in *Quon* also found that the text message pager service did not qualify as an RCS provider -- despite the fact that the provider archived messages on its server -- because the provider allowed users to send and receive electronic communications and any storage of messages was for backup purposes and was a "temporary, immediate storage of communications incidental to the electronic transmission thereof." *Crispin*, 717 F. Supp.2d at 978-79 (citing Theofel v. Farey-Jones, 359 F.3d 1066, 1070 (9th Cir. 2004) and 18 U.S.C. § 2510(17)).

[29] 359 F.3d 1066 (9th Cir. 2004).

[30] *Crispin*, 717 F. Supp.2d at 979-80.

[31] *Crispin*, 717 F. Supp.2d at 980.

[32] 18 U.S.C. § 2702(a)(1).

[33] 18 U.S.C. § 2702(a)(1); 18 U.S.C. § 2510(17).

[34] *Crispin*, 717 F. Supp.2d at 973 (quoting 18 U.S.C. § 2702(a)(1) and (2)).

[35] *Crispin*, 717 F. Supp.2d at 987. Note also that the *Crispin* court was not presented with facts about the three sites' storage of communications on their own private servers; instead, the court only dealt with communications that were retained by Crispin. However, with respect to storage on servers beyond that which was available to Crispin, the court noted "such archived copies [of messages] would plainly be for backup purposes." 717 F. Supp.2d at 987, FN 46.

[36] Both Facebook and MySpace allow users to post comments on other users' profile pages (*e.g.*, Facebook wall postings) which are not private person-to-person messages but are instead viewable by a group of other users. "Facebook wall postings and the MySpace comments are not strictly 'public,' but are accessible only to those users plaintiff selects." *Crispin*, 717 F.3d at 980.

[37] *Crispin*, 717 F. Supp.2d at 980-81.

[38] *Id.* (citing, e.g., U.S. v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003), Konop v. Hawaiian Airlines, Inc., 302 F.3d 874, 875 (9th Cir. 2002)).

[39] *Crispin*, 717 F. Supp.2d at 989.

[40] *Id.*

[41] *Crispin*, 717 F. Supp.2d at 989.
[42] *Id.* at 990 (citing Viacom International Inc. v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y.2008)).
[43] *Crispin*, 717 F. Supp.2d at 990.
[44] *Id.* at 991.
[45] *Crispin*, 717 F. Supp.2d at 972 (quoting William Jeremy Robison, Note, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1198 (2010)).
[46] *Crispin*, 717 F. Supp.2d at 972 (quoting *Konop*, 302 F.3d at 874).
[47] Seligstein, *supra* note 3.
[48] *Crispin*, 717 F. Supp.2d at 974-75.
[49] *Id.* at 975 (quoting Robison, *supra* note 45 at 1208-09 (footnote omitted)).
[50] A government entity, "after fulfilling certain procedural and notice requirements, [can] obtain information from an RCS provider via administrative subpoena or grand jury or trial subpoena." *Crispin*, 717 F. Supp.2d at 974-75 (citing 18 U.S.C. § 2703(b)). The SCA also "permits a governmental entity to obtain information from an ECS provider only pursuant to criminal warrant if the communication has been held by the provider for fewer than 180 days. In all other cases, the governmental entity can obtain information from an ECS provider using the subpoena procedures set forth in § 2703(b)." *Crispin*, 717 F. Supp.2d at 975.
[51] *See*, *e.g.*, Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 655-54 (N.Y. Sup. Ct. 2010) (granting defendant's motion to compel disclosure of public portions of plaintiff's Facebook and MySpace pages and noting that defendant's need for the information outweighed plaintiff's privacy concerns).

United States National Security: Biometrics and Privacy in Iraq

By Leta Gorman and John Spomer

"Sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists."

"For terrorists, travel documents are as important as weapons."

-- The 9/11 Commission Report

"ON September 11, 2001, 19 terrorists boarded aircraft in Boston, Massachusetts and Dulles, Virginia and changed our world. All had successfully passed through security screening prior to boarding the aircraft and, previously, had also successfully passed through immigration screening while entering the country. A suspected 20th terrorist had been refused entry by a suspicious immigration inspector at Florida's Orlando International Airport the previous month. Of the remaining 19 terrorists, 18 had been issued U.S. identification documents. The global war on terror had reached American soil, and the terrorists had already realized how important identify was to be in this fight."[1]

I. Introduction

The tragic events of September 11, 2001 have generated much debate "over the extent to which individual privacy must give way in the quest for greater security."[2] On one side of the debate are those who believe that essential liberties, such as privacy, must never be given up or compromised. On the other side are those who believe that the threat of terrorists operating in the U.S., who have access to weapons capable of causing incredible destruction, require that Americans lower their expectations of privacy.

This debate over the right to privacy versus concerns of national security has extended overseas to include the privacy rights of citizens of other countries. In

Leta Gorman is a shareholder in Bullivant Houser Bailey, P.C.'s Portland, Oregon office, where her practice focuses on the defense of manufacturers of consumer and industrial products. Leta is a member of the International Association of Defense Counsel ("IADC"). She is a frequent speaker at local and national legal conferences, including the 2010 IADC Corporate Counsel College. She also served on the faculty of the 2010 IADC Trial Academy. Leta received her undergraduate degree from the University of Washington, Jackson School of International Studies, where she focused on U.S. Foreign Policy and Diplomacy.

John Spomer is a senior associate Bullivant Houser Bailey, P.C.'s Sacramento, California office. His practice focuses on both commercial litigation and general business transactions, with particular emphasis on mergers and acquisitions, corporate governance, corporate formations and financing and commercial leasing.

Iraq, for over four years now, U.S. military troops have been using scanners to collect the fingerprints, iris scans and other personal information of millions of Iraqi civilians. This data is then stored in a central database that can be used to protect the national security of the U.S. by locating possible suspects in past and future terrorist attacks. The system of collecting this information, called "biometrics," is at the center of a controversy that several human rights groups are concerned is putting the lives of many Iraqis at risk on a daily basis.

Most, if not all, Americans will agree that U.S. national security and the protection of U.S. citizens is of critical import. After discussing the nature of biometrics generally, the article will discuss the current use of biometrics in Iraq by the U.S. military to ensure U.S. national security. The article then turns the focus on the privacy concerns of the Iraqi civilians who fear that the private biometric data collected by the U.S. to protect Americans will be used as a sort of a "hit list" against innocent Iraqi lives. Finally, the article proposes several "best practice" guidelines that should be carefully considered by the U.S. government in operating and maintaining a biometrics system in Iraq.

II. Biometrics and its Applications

Historically, the term "biometrics" has referred to the "development of statistical and mathematical methods applicable to data analysis problems in the biological sciences."[3] In 1948, R. A. Fisher defined "biometry" as "the active pursuit of biological knowledge by quantitative methods."[4] One example of biometrics is the use of statistical methods to analyze data from human clinical trials that evaluate the relative effectiveness of competing treatments for disease.[5] Another example involves the use of statistics to analyze data from environmental studies regarding the effects of pollution on the rate of human disease in a particular region.[6] Recently, however, the term "biometrics" has received mainstream recognition because of its reference to the emerging field of technology associated with the identification of individuals using biological traits, such as those based on fingerprints, retinal or iris scanning, or face recognition.[7]

Biometrics currently has several applications in the United States, both on governmental and commercial levels. For example, biometrics is currently used at United States' borders to ensure that persons who are a known threat are not allowed entrance. Specifically, the government utilizes a biometrics system, called "US-VISIT," designed to identify persons seeking entry into the United States who are a terrorist threat, while facilitating the flow of legitimate persons into and out of the country.[8] It contains fingerprints, photographs and biographical information on foreign persons entering the country through ports of entry, those apprehended by the Customs and Border Protection or Immigration and Customs Enforcement, persons deported from the U.S., persons who have applied for border crossing cards in Mexico, persons who have applied for asylum, and lookout data.[9] US-VISIT closely coordinates with other U.S. government agencies, such as the Department of Justice, to incorporate

information on foreign born individuals that are wanted for crimes or suspected of terrorism.[10] Upon arrival at a port of entry, the individual has finger scans and a photograph taken.[11] The purpose is to ensure that the person granted the visa is the same person attempting to gain entry with that visa.[12]

Additionally, U.S. passports with facial biometric data were scheduled to be issued beginning in 2005.[13] Technical difficulties, however, are delaying the integration of biometrics into passports in both the United States and European Union ("EU").[14] Some of these problems include the compatibility of reading devices, information formatting, and the nature of content (e.g. the United States and United Kingdom currently expect to use only image data, whereas the EU intends to use fingerprint and image data in their passport biometric chip(s)).[15]

On a commercial level, people are finding biometrics more prevalent than ever in their daily lives. 24 Hour Fitness, for example, recently introduced a cardless check-in system nationwide that uses fingerprint scans to identify members.[16] The company touted the cost savings and environmental benefits from not having to issue about 1 million plastic membership cards each year as an incentive to go with a fingerprint identification system.[17] Instead of electronically scanning and storing members' full fingerprints, the system charts the distance between certain ridges of a fingerprint and converts the information into a binary code that is encrypted.[18] To enter the club, a member places their finger on an electronic scanner and then enters a unique 10 digit code on a keypad, which, together, confirm the member's identity.[19] Moreover, the system itself is voluntary and members can still gain access to the club simply by showing their driver's license.[20] 24 Hour Fitness claims that customer response has been extremely favorable, including a 97% acceptance rate among members in its northern division.[21]

Walt Disney World® is responsible for the nation's largest single commercial application of biometrics.[22] At The Walt Disney World in Orlando, biometric measurements are taken from the fingers of multi-day pass users to ensure that the pass is used by the same person from day to day.[23] Privacy advocates criticize this usage of biometrics, arguing that it requires the customer to divulge too much personal information simply for access to roller coasters.[24] They also argue that Disney fails to fully disclose the purpose of its new system, citing that there are no signs posted at the entrances detailing what information is being collected and how it is being used.[25]

Disney, meanwhile, counters that the scanned information is stored "independent of all of our other systems" and "the system purges [the information] 30 days after the ticket expires or is fully utilized."[26] Visitors who object to the fingerprint scanners can provide photo identification instead, although the option is not advertised at the park entrances.[27] Although Walt Disney World in Orlando is the only Disney location to use this biometric technology at its entrances, other theme parks, such as Sea World and Busch Gardens, have begun to use similar technology.[28]

The federal government has taken notice of Disney's use of biometrics. In

fact, the federal government recently sought out Disney's advice in intelligence, security and biometrics.[29] One Disney executive was part of a group convened by the Federal Aviation Administration and other federal agencies to help develop a plan for "Passenger Protection and Identity Verification" at airports, using biometrics.[30] The executive, Gordon Levin, also was part of a group asked by the National Institute of Standards and Technology and the National Security Agency to develop national standards for the biometrics industry.[31]

Even when used on a solely commercial level, however, biometrics still poses a risk to an individual's security. Privacy activists in many countries have criticized the technology's use for the potential harm to civil liberties, privacy, and the risk of identity theft. When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. In 2005, for example, car thieves cut off the finger of a Mercedes owner when attempting to steal the car, which was protected by a fingerprint recognition system.[32]

In addition to collecting biometric information, many countries, including the United States, have begun trading biometric data. According to a recent article in *National Defense*, the United States Defense Department is under pressure to share biometric data and has bi-lateral agreements to share biometric data with about 25 countries.[33] In fact, every time a foreign leader has visited Washington, D.C. over the past few years, the federal government has made sure that the leader enters into such an agreement.[34]

Despite the concerns about safeguarding biometric information, the use of biometrics continues to spread worldwide. The United Kingdom uses biometrics in some of its schools as a quick way for children to subtract money from lunch spending accounts.[35] And in Germany, the biometrics business has grown from about $15 million in 2004 to more than $400 million last year.[36] Germany was also one of the first countries to implement biometric technology at the Olympic Games to protect German athletes.[37] At the Olympic Summer Games in Athens, Greece in 2004, accredited visitors to the German Olympic village (*e.g.*, athletes, coaching staff, team management and members of the media) received an identification card containing their fingerprint biometrics data, which enabled them to access the "German House."[38]

III. Biometrics and its Impact on Iraq

Biometrics in Iraq has a far more significant impact than its use at theme parks and gyms. For nearly 1,500 years, the Sunni and Shiite Muslims have been engaged in an open and bloody conflict. As the two major denominations of Islam, it is estimated that 80-90% of the world's Muslims are Sunni and 10-20% are Shiite.[39] Shiites, however, make up the majority of the population in Iraq.[40] The historic background of the Sunni–Shiite split lies in the schism that occurred when

the Islamic prophet Muhammad died in the year 632 AD, leading to a dispute over succession to Muhammad as a caliph of the Islamic community spread across various parts of the world, which led to the Battle of Siffin.[41] Sectarian violence persists to this day in Iraq and has become particularly heightened since the United States' invasion.[42]

Because there is no way to physically tell a Sunni Arab from a Shiite Arab, militiamen and insurgents are increasingly killing people based on common identification factors, such as a person's name or whether that person resides in a province dominated by one particular group.[43] In June 2006, Sunni gunmen dragged students from a bus, identified and separated the Sunnis from the group, and then killed the 21 remaining Shiites.[44] A month later, Shiite gunmen set up fake checkpoints in Baghdad, dragged up to 50 people from their cars and killed them after checking their identification cards.[45] Accordingly, a growing number of Iraqis are changing their names to conceal their particular sect, many choosing "neutral" names such as Ahmed or Muhammed.[46] After the bombing of a Shiite shrine in 2006 set off a wave of sectarian violence, over 1,000 Iraqis officially changed their names.[47]

Despite the highly sensitive nature of an Iraqi's name and residence, the U.S. military has been collecting the personal information of Iraqi civilians in an attempt to identify suspects in terror attacks and stabilize various regions in the country.[48] To do so, the U.S. military began using mobile scanners in about 2007 to gather fingerprints, iris scans and other personal data from Iraqi civilians at checkpoints, attack sites, workplaces and even homes.[49] Today, there are at least three biometrics systems in operation in Iraq: (1) the Automated Fingerprint System, (2) the Biometrics Automated Toolset, used to identify residents of a particular city, and (3) the Biometric Identification System for Access, used for access to military and diplomat zones.[50] Personal information in the database includes an individual's name, parents' names, address, birth data, height and weight.[51] The information collected from these biometric systems is then stored in a central database inside the Pentagon's Biometric Fusion Center.[52] The database is administered by the U.S. military and can be accessed by certain individuals within Iraq's Interior Ministry and a limited number of American contractors.[53]

The identification information in the database is used to help track suspected militants and identify suspects in attacks both on U.S. troops and Iraqi civilians.[54] Every military squad in Iraq is now equipped with an electronic scanner that can collect the records of up to 10,000 people and display identification data, allowing troops to view a person's background and decide whether he or she should be detained.[55] The information downloaded by the scanners is forwarded to the central database, maintained by the military, and includes records of Iraqis who have been detained or who work in U.S. facilities or for the Iraqi army or police.[56] That data can be compared to fingerprints found at attack sites to find potential suspects.[57]

Compliance with the biometric system in Iraq is effectively mandatory. U.S. troops have ordered Iraqi civilians,

including children, out of their villages to record their fingerprints and iris scans before allowing them to return.[58] Iraqis who refuse to give data can be blocked from neighborhoods, markets or other places that require identification for entry.[59] As one military commander remarked, however, "virtually nobody refuses."[60]

After years of compiling information into its database, the U.S. military now has identification information on more than 2.5 million Iraqis.[61] Lisa Swan, the deputy director of the U.S. Army's Biometric Task Force says that this biometric identification database has allowed U.S. troops to capture more than 400 "high-value individuals" in Iraq and Afghanistan over a one year period alone.[62]

In March 2007, the Defense Science Board ("DSB") issued its report on Defense Biometrics to the U.S. Department of Defense.[63] The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense.[64] The report focused on issues surrounding the use of biometrics in the Department of Defense, not only in Iraq, but worldwide.[65] Specifically, the 168 page report discusses biometric information management and sharing, research and development, technology, organizational issues and legal and privacy issues.[66] In acknowledging the various privacy risks involved with a biometric system, the report expressed "the clear need for the establishment of uniform constructs in complex areas of unsettled law and policy related to biometrics, and privacy is a good place to start."[67] It also encouraged the Department of Defense to "emphasize the opportunity for improved security and audit controls in a centralized structure" to offset many privacy concerns.[68] The report goes on to discuss to discuss specific issues related to identity theft and biometrics.[69]

In general, the DSB report illustrates some of the significant, touchstone issues and makes numerous recommendations as to how a vast biometric database should be maintained and safeguarded by the U.S. government. To facilitate the current operation of the biometric database, President George W. Bush issued Homeland Presidential Security Directive 24 ("HSPD-24") on June 5, 2008.[70] The purpose of the directive was to establish a "framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection storage, use, analysis, and sharing of biometric [information]."[71] HSPD-24 also calls for the privacy protection of individuals under U.S. law, stating, "All agencies shall execute this directive in a lawful and appropriate manner, respecting the information privacy and other legal rights of individuals under United States law, maintaining data integrity and security, and protecting intelligence sources, methods, activities, and sensitive law enforcement information."[72] Finally, HSPD-24 required the Attorney General to create an "action plan" to implement the purpose and goals of the directive, including how "the information privacy and other legal rights of individuals" would be protected.[73] It is unknown, however, whether this action plan was ever created or, if so, its contents.

As for the future use of biometrics in Iraq after the U.S. military departs, the

idea of turning over the database system to the Iraqi government is already being considered. The Council on Foreign Relations ("CFR"), an independent, nonpartisan membership organization and "think tank," has proposed a national identification program that would provide Iraqis with identification cards, similar to U.S. drivers' licenses, with biometric data like fingerprints to be presented at security checkpoints.[74] Combined with the existing biometric database system, the identification cards would help "identify insurgents who blend in with the civilian population."[75] Several problems potentially exist with this plan, however. First, there is the aforementioned problem that the database could fall into the wrong hands and be used for ethnic cleansing.[76] Another problem is the fact that an estimated four million Iraqis are either internally displaced or living as refugees abroad and would not get identification cards, effectively denying them citizenship in their own country.[77] There are also issues regarding trusting the Iraqi government with the vast amount of sensitive information contained in the biometric database and whether the country can afford to operate and maintain it.[78]

The current protocols and safety procedures designed to protect Iraqi civilians from the misuse of the vast amount of private information store in the biometric database is either unknown or non-existent. Moreover, a plan to ultimately transition the database information to the Iraqi government with effective safeguards and procedures to protect the privacy of the information contained in the system also does not exist. Given the potential for catastrophic consequences should protective measures not be taken, it is paramount that specific issues relating to the operation and use of the biometric database be considered and addressed as soon as possible.

IV. Proposals for Establishing Security Measures over Biometric Information in Iraq.

The issue of privacy and securing the identities of Iraqi civilians captured and stored by a biometrics database is of immediate importance. In addition to the factors previously discussed, the technology of biometrics and its wide variety of uses is growing considerably faster than the policies related to its usage and consequences. As stated in the DSB report, "Effective security safeguards for storage and use of biometrics information are simply indispensible, and security breaches in this area will be more than embarrassing. Due to the enormous importance that the Task Force attaches to biometrics generally, the future in this area is simply too important to risk negative (or legislative!) reaction to avoidable errors."[79]

Before examining proposals for safeguarding the private information contained in the biometric database, the proper agency or authority to promulgate these rules should be determined. Recognizing the desire to establish guidelines that can be followed both by the United States, currently, and Iraq, in the future after the database is turned over to its government, it is tempting to first consider an international body to oversee the adoption and adherence to these rules. The United Nations may seem like a

particularly likely candidate. Its ability to draft a treaty or other set of rules with respect to such a specific issue and, even more importantly, its ability to enforce those rules, is doubtful in light of history, however.

For example, the International Covenant on Civil and Political Rights ("ICCPR") is a multilateral treaty adopted by the United Nations General Assembly on December 16, 1966, which has been in force since March 23, 1976.[80] It commits its parties to respect the civil and political rights of individuals, including the right to life, freedom of religion, freedom of speech, freedom of assembly, electoral rights and rights to due process and a fair trial.[81] Article 17, in particular, mandates an individual's right of privacy.[82] The United Nations High Commissioner for Human Rights clarified that this right to privacy includes personal information stored on computers and databanks, that parties must take effective measures to protect against unauthorized access to this information, and that this information is never used for purposes incompatible with the treaties.[83] The United States, however, ratified the ICCPR subject to the non-self-execution declaration so that it does not form part of the domestic law of the nation, effectively removing any obligation of the U.S. to comport with any of the covenant's principles.[84]

For the present time, the Department of Defense, which currently oversees the existing biometric database in Iraq, should not only promulgate specific procedures to protect against the unauthorized access and disclosure of Iraqis' personal information, but it must also set up controls within the biometric system that will continue to protect the right of privacy of these people when the system is turned over to the Iraqi government. The DSB report suggests that the Office of the General Counsel, with assistance from the Department of Justice, should review the privacy implications of biometrics within the Department of Defense.[85] The results can then be used by the Office of the Secretary of Defense to create comprehensive biometrics privacy policies.[86]

Although proposals for a specific set of rules relating to the entire biometric system is outside the scope of this article, it is helpful to examine certain "best practices" previously proposed by the International Biometric Group ("IBG") and which have particular relevance to the privacy situation in Iraq.[87] IBG groups these best practices into four categories: (1) scope and capabilities, (2) data protection, (3) user control of personal data, and (4) disclosure, auditing, accountability, and oversight.[88]

Within the category of *Scope and Capabilities*, particular emphasis in the use of a biometrics system in Iraq should focus on limiting the scope of the information gathered, as well as a careful analysis of the scope of the system's actual and *potential* capabilities, such that all of the system's risks can be evaluated and addressed.[89] The DSB report places particular emphasis on communicating and understanding the purpose of the biometric system and limiting the data collected to that purpose alone.[90]

Given the widespread sectarian violence in Iraq, the category of *Data Protection* is potentially the most significant in attempting to ensure the safety of civilians from the unintended

consequences of a biometrics system. Several methods can be deployed to help best ensure that biometrics data is kept secure. For example, not only does the information itself need to be protected from theft but the means of transmitting that data must also be kept secure.[91] In addition, the system functions and data must be limited to certain personnel under certain conditions, with explicit controls on usage and export set in the system.[92] The biometric data also should be kept separate from personal information about the individual, including the person's name and address.[93] Finally, a method should be established by which a system used to commit or facilitate privacy-invasive biometric matching, searches, or linking "can be depopulated and dismantled."[94] The responsibility for making such a determination may rest with an independent auditing group, outside of the Department of Defense, and would be subject to appropriate appeals and oversight.[95]

The third category regarding *User Control of Personal Data* is more difficult to achieve in insurgent areas, such as Iraq, where there is a compelling interest for data to be retained for verification or identification purposes, such that the option of unenrollment would render the system inoperable.[96]

The final category involving the *Disclosure, Auditing, Accountability, and Oversight* of the biometrics system is of crucial significance in attempting to develop protections of an individual's privacy in Iraq. The centerpiece of this category is the creation of an independent auditing body to ensure adherence to standards regarding data collection, storage, and use.[97] In addition, the data derived from such oversight should be available "to facilitate public discussion on the system's privacy impact."[98] As a prerequisite to operating the biometric system, it should be clearly stated who is responsible for system operation, to whom questions or requests for information are addressed, and what recourse individuals have to resolve their grievances.[99] Individuals should also be informed of any protections being taken to secure biometric information, "including encryption, private networks, secure facilities, administrative controls, and data segregation."[100]

Finally, in addition to formulating rules and guidelines to protect the privacy of Iraqi civilians, legal procedure issues must also be considered. For example, the evidentiary value, acceptance and standard of application of biometrics measurements and identification must be known before it is allowed in court.[101] As the DSB noted, "In a counterinsurgency operation, like Iraq, the biometrics identity system, how it functioned, where it resided, who was in it and the standards by which that occurred was not known or regarded as significant."[102] Accordingly, established legal procedures need to be set in place in Iraq so that biometric data recovered from a device, weapon, document, or other instrument is handled and presented in such a way as to support the identification and prosecution of suspected insurgents in court.[103]

In conclusion, it is important to bear in mind a critical recommendation stated in the DSB report, namely that privacy considerations be incorporated into the design of any human identification system at an early stage.[104] The U.S.

military has already been using a comprehensive biometric system and database in Iraq for nearly four years. Yet it is uncertain whether any regulations, or even suggested "best practices," exist to protect Iraqis from the potential deadly misuse of the personal information contained in the system. The right to privacy exists as a fundamental freedom enjoyed by American citizens in this country. Today, Americans increasingly are aware of the government's impact on their individual privacy rights, as it seeks to protect these very same freedoms from future terrorist actions. Now, however, it is time for the United States to be vigilant in safeguarding these same basic rights enjoyed by citizens a half world away, whose freedom for which this government is also fighting.

---

[1] National Science and Technology Council, *BIOMETRICS in Government Post – 9/11, Advancing Science, Enhancing Operations*, August 2008, http://www.biometrics.gov/Documents/Biometrics%20in%20Government%20Post%209-11.pdf.

[2] Fred H. Cate, *Information Privacy in the War on Terrorism*, White Paper, October 18, 2007. http://web1.millercenter.org/debates/whitepaper/deb_2007_1113_privacy.pdf.

[3] *Definition of Biometrics*, BIOMETRICS, A JOURNAL OF THE INTERNATIONAL BIOMETRIC SOCIETY, http://www.biometrics.tibs.org/ (last visited Dec. 7, 2010).

[4] R. A. Fisher, *Biometry*, BIOMETRICS, 1948, at 218.

[5] *Definition of Biometrics*, BIOMETRICS, A JOURNAL OF THE INTERNATIONAL BIOMETRIC SOCIETY, http://www.biometrics.tibs.org/ (last visited Dec. 7, 2010).

[6] *Id.*

[7] *Id.*

[8] DEFENSE SCIENCE BOARD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE BIOMETRICS 131 (2007).

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Biometrics*, NEW WORLD ENCYCLOPEDIA (AUG. 29, 2008), http://www.newworldencyclopedia.org/entry/Biometrics#United_States.

[14] *Id.*

[15] *Id.*

[16] Steve Raabe, *Fitness Club's Fingerprint Entry System Pumps Up Debate Over Biometric Identity*, THE DENVER POST, November 14, 2010, http://www.denverpost.com/headlines/ci_16601571.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Karen Harmel, *Walt Disney World: The Government's Tomorrowland?*, NEWS 21, September 1, 2006, http://newsinitiative.org/story/2006/09/01/walt_disney_world_the_governments.

[23] The Canadian Press, *Disney: It's A Secure World After All*, CBC NEWS, September 5, 2006, http://www.cbc.ca/technology/story/2006/09/05/tech-disney.html.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] Karen Harmel, *Walt Disney World: The Government's Tomorrowland?*, NEWS 21, September 1, 2006, http://newsinitiative.org/story/2006/09/01/walt_disney_world_the_governments.

[30] *Id.*

[31] *Id.*

[32] Jonathan Kent, *Malaysia Car Thieves Steal Finger*, BBC NEWS, March 31, 2005, http://news.bbc.co.uk/2/hi/asia - pacific/4395831.stm.

[33] Stew Magnuson, *Defense Department Under Pressure To Share Biometric Data*, NATIONAL DEFENSE, January 2009, http://www.nationaldefensemagazine.org/archive/2009/January/Pages/DefenseDepartmentUnderPressuretoShareBiometricData.aspx.

[34] *Id.*

[35] Laura Emerson, *Biometrics Company Brings New Level Of Protection To Las Vegas Businesses*, LAS VEGAS BUSINESS PRESS, November 22, 2010, http://www.lvbusinesspress.com/articles/2010/11/22/news/iq_39814564.txt.

[36] United Press International (UPI), *Biometrics Seen As Ultimate Secure ID*, UPI.COM, November 24, 2010, http://www.upi.com/Business_News/Security-Industry/2010/11/24/Biometrics-seen-as-ultimate-secure-ID/UPI-13281290633916/.

[37] Will Sturgeon, *Biometrics Used To Keep German Olympians Safe*, SILICON.COM, August 11, 2004, http://www.silicon.com/technology/security/2004/08/11/biometrics-used-to-keep-german-olympians-safe-39123078/.

[38] *Id.*

[39] THE PEW FORUM ON RELIGION AND PUBLIC LIFE, MAPPING THE GLOBAL MUSLIM POPULATION, 8 (2009).

[40] *Id.*

[41] FEBE ARMANIOS, CONGRESSIONAL RESEARCH REPORT FOR CONGRESS, ISLAM: SUNNIS AND SHIITES, CRS-2-3 (2004).

[42] *Iraq 101: Civil War*, MOTHER JONES, March 1, 2007, http://motherjones.com/politics/2007/03/iraq-101-civil-war.

[43] Edward Wong, *To Stay Alive, Iraqis Change Their Names*, THE NEW YORK TIMES, September 6, 2006, http://www.nytimes.com/2006/09/06/world/middleeast/06identity.html.

[44] Yahya Barzanji, *Gunmen Kill 21 In Iraq, Many Of Them Students*, THE WASHINGTON POST, June 4, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/04/AR2006060400155.html.

[45] Edward Wong, *To Stay Alive, Iraqis Change Their Names*, THE NEW YORK TIMES, September 6, 2006, http://www.nytimes.com/2006/09/06/world/middleeast/06identity.html.

[46] *Id.*

[47] *Id.*

[48] In October 2005, the Iraqi constitution was approved. Article 17 of the Constitution sets forth two limited privacy rights. First, "Every individual shall have the right to personal privacy so long as it does not contradict the rights of others and public morals." Second, "The sanctity of the homes shall be protected. Homes may not be entered, searched, or violated, except by a judicial decision in accordance with the law." Art. 17, Fed. Rep. of Iraq Const. (2005). The Iraqi armed forces frequently did respect these privacy rights. Iraqi armed forces regularly searched homes, workplaces, and individuals without first obtaining a warrant or having probable cause. Those captured in these searches were then indefinitely detained incommunicado. US State Dept., Human Rights Report 2006 – Iraq (March 6, 2007), http://www.state.gov/g/drl/rls/hrrpt/2006/78853.htm.

[49] Thomas Frank, *U.S. Is Building Database On Iraqis*, USA TODAY, July 12, 2007, http://www.usatoday.com/news/world/iraq/2007-07-12-iraq-database_N.htm.

[50] Jonathan E. Skillings, *Biometrics And Security In Iraq*, CNET NEWS, August 17, 2007, http://news.cnet.com/8301-10784_3-9761654-7.html.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] Thomas Frank, *U.S. Is Building Database On Iraqis*, USA TODAY, July 12, 2007, http://www.usatoday.com/news/world/iraq/2007-07-12-iraq-database_N.htm.

[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] William Matthews, *Double-Edged Sword: U.S. Biometric Database Yields Rewards – And Risks*, DEFENSE NEWS, August 24, 2009, http://www.defensenews.com/story.php?i=4246877.
[59] Thomas Frank, *U.S. Is Building Database On Iraqis*, USA TODAY, July 12, 2007, http://www.usatoday.com/news/world/iraq/2007-07-12-iraq-database_N.htm.
[60] *Id.*
[61] William Matthews, *Double-Edged Sword: U.S. Biometric Database Yields Rewards – And Risks*, DEFENSE NEWS, August 24, 2009, http://www.defensenews.com/story.php?i=4246877.
[62] *Id.*
[63] DEFENSE SCIENCE BOARD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE BIOMETRICS (2007).
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.* at 71.
[68] *Id.* at 70.
[69] *Id.* at 72-82.
[70] Homeland Security Presidential Directive 24: Biometrics for Identification and Screening to Enhance National Security, 2008 WEEKLY COMP. PRES. DOC. 788 (June 5, 2008).
[71] *Id.*
[72] *Id.* at 790.
[73] *Id.* at 791.
[74] Lionel Beehner, *Backgrounder: A National ID Program For Iraq?*, THE NEW YORK TIMES, May 29, 2007, http://www.nytimes.com/cfr/world/slot2_20070529.html.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] DEFENSE SCIENCE BOARD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE BIOMETRICS 69 (2007).
[80] International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force Mar. 23, 1976.
[81] *Id.*
[82] *Id.*
[83] General Comment No. 16 from the Office of the High Commissioner for Human Rights: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17) (April 8, 1988), http://www.unhchr.ch/tbs/doc.nsf/0/23378a8724595410c12563ed004aeecd?Opendocument.
[84] 138 CONG. REC. S4781-84 (daily ed. Apr. 2, 1992); S. EXEC. REP. NO. 102-23, at 15 (1992).
[85] DEFENSE SCIENCE BOARD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE BIOMETRICS 72 (2007).
[86] *Id.*
[87] *IBG BioPrivacy Initiative: Best Practices For Privacy-Sympathetic Biometric Deployment*, International Biometric Group, LLC, http://www.bioprivacy.org/ (last visited December 8, 2010).
[88] *Id.*
[89] *Id.*
[90] DEFENSE SCIENCE BOARD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE BIOMETRICS 72 (2007).
[91] *IBG BioPrivacy Initiative: Best Practices For Privacy-Sympathetic Biometric Deployment*, International Biometric Group, LLC, http://www.bioprivacy.org/ (last visited December 8, 2010).
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] DEFENSE SCIENCE BOARD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE BIOMETRICS 130 (2007).
[102] *Id.*
[103] *Id.*
[104] *Id.* at 71.

Privacy in the Petition Process - Signing Your Privacy Away?

By Lauren A. Shurman, Monica S. Call, and John A. Anderson

NEARLY half the states in the United States have a petition or referendum process for citizens to directly make or repeal laws. This form of direct democracy has interesting First Amendment implications because petition signers have particular associational rights they might like to protect by keeping their names private. Most state disclosure laws, however, permit the public disclosure of the names of petition signers. Those that fear the loss of privacy through the disclosure of petition signatures lament that that disclosure laws—originally meant to prevent fraud and promote confidence in the democratic process—now equip political opponents with a tool to harass and intimidate, thereby discouraging participation in the democratic process. For these groups, signing a petition should be just as private as casting a secret ballot. In contrast, those who seek full disclosure argue that signing a petition is a public, legislative act. In their view, disclosure is necessary to prevent fraud and creates a more informed electorate. The application of state disclosure laws to the electoral process has broad implications for privacy rights in general, especially in this age of instantaneous information, where the Internet is the new political battleground.

Lauren A. Shurman, a 2006 graduate of Duke University School of Law, and Monica S. Call, a 2004 graduate of Stanford Law School, are both litigation associates in the Salt Lake City office of Stoel Rives, LLP.

IADC member John A. Anderson, a 1981 graduate of University of Virginia School of Law, is a litigation partner in the Salt Lake City office of Stoel Rives, LLP. *Special thanks to Brigman L. Harman for his excellent editorial assistance.*

The recent United States Supreme Court case of *Doe v. Reed* highlights the tension between these interests in the Digital Age. In *Doe v. Reed*, the Court upheld Washington State's disclosure laws against a First Amendment facial challenge. The Court held that the government's interest in preserving the integrity of the electoral process permitted it to disclose the names of those that sign petitions. In that case, the petition signers feared harassment and intimidation if their names were made public by the state and converted into an electronic searchable format by their political opponents. The decision left open the question of whether the petition signers might succeed on their as-applied challenge.

The Court's opinion in *Doe v. Reed* and its guidance to lower courts that will be faced with as-applied challenges to disclosure laws demonstrates the delicate balance of privacy rights in the electoral context.

I. Background on State Initiative and Referendum Processes

The initiative and referendum are "direct democracy" measures by which citizens can place statutes and constitutional amendments on the ballot. An initiative allows citizen-initiated statutes or constitutional amendments to be placed on the ballot after a certain number of signatures are collected on a petition. Twenty-four states currently allow for some form of an initiative (18 states allow constitutional amendments by initiative, and 21 states allow statutes by initiative).[1] Initiatives are also commonly used by local and city governments. A referendum, by contrast, is a citizen-initiated proposal to repeal a law that was previously enacted by the legislature. Like an initiative, a referendum is placed on the ballot after a threshold number of signatures is gathered on a petition. Twenty-four states currently allow for referendums, though referendum use is less common than initiative use.[2] Of the twenty-four states that allow initiatives and referendums, all but California treat the petitions used to gather signatures as public records under the states' public records statutes or "sunshine laws."[3]

The initiative and referendum processes were first promoted in the United States, mostly in the west, during the Progressive Era beginning in the 1890's.[4] The Progressives, who felt as though the representative form of government was out of touch with the citizens and controlled by special interest groups, borrowed the initiative and referendum process from the Swiss constitution.[5] The first state to place a statewide initiative on the ballot was Oregon, in 1904.[6] The use of initiatives surged during the early part of the twentieth century, but then dropped off with the advent of World War I and the Great Depression.[7] The initiative movement was reignited in 1978, when California voters passed Proposition 13, which capped property taxes in the state to just 1 percent.[8] After that, the use of the initiative and referendum process grew steadily, reaching a high point in 1996.[9] In 1996, citizens placed 93 initiatives on statewide ballots, 47% of which were approved by voters.[10] In total, since Oregon's first statewide initiative in 1904, 2,356 state-level initiatives have been sent to the ballot, and approximately 41% have been approved by voters.[11]

II. Privacy and Voting

Although every state currently provides a secret ballot for voters, the states did not begin to adopt the secret ballot until the late 1800's.[12] The secret ballot was adopted primarily as a means to combat abuses in the voting process because the public means of voting previously employed by the states fostered voter coercion and bribery.[13]

Constitutional protections for secrecy or privacy in voting and political activity have gradually worked their way into First Amendment jurisprudence, primarily through the First Amendment's right of freedom of assembly, which the Supreme Court has recognized encompasses a right of freedom of association.[14] In 1958, the Supreme Court in *NAACP v. Alabama*, recognized a "vital relationship between freedom to

associate and privacy in one's associations."[15] The Court held that the NAACP's right to withhold its membership lists from the state was "so related to the right of the members to pursue their lawful private interests privately and to associate freely with others" so as to come within the protection of the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.[16] The Court found this to be the case in light of the NAACP's evidence that its members had been subject to hostility and economic and physical threats, such that disclosure of its membership list would be likely to dissuade individuals from joining the association.[17]

Since *NAACP v. Alabama*, the Court has reiterated the importance of privacy in promoting First Amendment interests.[18] In *Buckley v. Valeo*, the Court noted that compelled disclosure of political speech "can seriously infringe on privacy of association and belief guaranteed by the First Amendment."[19] The Court again noted in *Brown v. Socialist Workers '74 Campaign Committee* that "privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[20] Several years later, in *McIntyre v. Ohio Elections Commission*, the court acknowledged that the decision to remain anonymous in advancing political causes was "an aspect of the freedom of speech protected by the First Amendment" and that the tradition of anonymity was "perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation."[21]

Because of the importance of privacy and anonymity to First Amendment interests, the Court has subjected laws that seek to compel the disclosure of political speech to "exacting scrutiny."[22] Under this level of scrutiny, for a disclosure requirement to pass muster, there must be a substantial relation between the disclosure requirement and a sufficiently important governmental interest.[23] Applying the exacting scrutiny standard, the Court has struck down laws that banned the right to distribute anonymous leaflets[24] and that required petition gatherers to wear name tags,[25] while upholding the Federal Election Campaign Act's campaign contribution disclosure requirements[26]. While acknowledging that each of the disclosure requirements at issue in those cases had the potential to chill political speech, the Court reached different outcomes based on how strongly the Court perceived the relationship between the government's justification for the law and the information required to be disclosed. In *Buckley v. Valeo*, the Court found that the Federal Election Campaign Act's requirement that the names, addresses, and occupations of campaign contributors be made public was sufficiently related to the state's interests in providing the electorate with information about political candidates, deterring corruption by exposing large contributions and expenditures, and in detecting violations of campaign contribution limits.[27] In *McIntyre*, by contrast, the Court held that a law that barred anonymous political leaflets was not sufficiently related to the state's interests in informing the electorate and preventing fraud and libel.[28] With respect to the state's

informational interest, the Court held that compelling disclosure of the speaker's identity did not add sufficient information to the leaflet and that "[p]eople are intelligent enough to evaluate the source of an anonymous writing."[29] With respect to the state's interest in preventing fraud or libel, the Court found that other provisions in the election code sufficiently protected these interests.[30] Similarly, in *Buckley v. ACLF*, the Court held that a law that required individuals handing out petitions to wear name tags was not sufficiently related to the state's interests in administrative efficiency, fraud detection, and informing voters, especially because the state could meet those interests through other means that did not subject the petition circulators to "heat of the moment harassment," as wearing a name badge might.[31]

The Court has also acknowledged that the government's interest in compelled disclosure is "diminished" when dealing with minor political parties, which are less likely to have a sound financial base, more likely to fear reprisal, and are therefore more vulnerable to the chilling effect that compelled disclosure could have.[32] Minor parties, however, are not per se exempt from compelled disclosure laws. Rather, minor parties may bring an as-applied challenge to such laws. By demonstrating "a reasonable probability that the compelled disclosure of a party's contributors' names will subject them to threats, harassment, or reprisals from either Government officials or private parties," a minor party may obtain an exemption from a compelled disclosure law.[33]

In sum, the "compelled disclosure" line of cases from the Supreme Court suggests that the Court is willing to accept disclosure requirements, which inevitably result in a slight reduction in the quantity of speech and the speakers' privacy, but only when doing so will enhance the overall quality of political speech and serve the government's interest in regulating the election process. This analysis necessarily involves an empirical weighing of costs and benefits that makes outcomes somewhat difficult to predict.

Issues surrounding the interplay between privacy and voting and other political speech have come to the forefront recently with the increasing use of the Internet to disseminate information about voters' activities. Websites, such as FundRace, provide information to the general public about federal campaign contributions in a searchable format.[34] FundRace claims to "make[] it easy to search by name or address to see which candidates or political parties your friends, family, co-workers, and neighbors are contributing to."[35] Many states offer "Am I registered to vote?" services on their websites, in which any user can type in an individual's name and zip code or county to see if that individual is registered to vote and oftentimes whether they are a registered Democrat or Republican.[36] For a fee, other websites advertise that they can provide voter information to political campaigns, including information about party affiliation, frequency of voting, and the ethnicity of registered voters.[37]

Privacy concerns become heightened when these types of websites are targeted towards controversial ballot measures, such as California's recent Proposition 8, the state ballot measure defining marriage as only between a man and a woman. Under California's campaign finance

disclosure law, information about anyone who contributed more than $100 to Proposition 8 was made public, including the contributors' name, zip code, amount donated and, if the donor specified, employer.[38] An anonymous group collected this information about contributors and overlaid it with a Google map at a website called eightmaps.com.[39] Using this website, the identity and location of Proposition 8 supporters is made readily available to the public. Supporters of the website argue that it empowers Proposition 8 opponents to exercise their First Amendment rights by, for example, boycotting businesses that supported Proposition 8 and by engaging in debate with their neighbors who may appear on the website. But even proponents of state disclosure laws were uneasy about eightmaps.com.[40] Many contributors who appeared on the website complained that they were subject to harassment as a result.[41] As the *New York Times* commented, "The site pits … cherished values against each other: political transparency and untarnished democracy versus privacy and freedom of speech."[42] Indeed, although campaign disclosure laws were intended to enhance the political process by providing voters with helpful information about candidates, the use of such disclosure laws in unintended ways, such as with eightmaps.com, may now threaten the very process it was intended to promote by making some citizens afraid to participate in the political process for fear of reprisal.

III. *Doe v. Reed*

The interplay between a state's disclosure laws, the initiative and referendum process, and technological advancements all came to a head in the recent *Doe v. Reed* case. Like other cases the Court has faced recently, and will certainly face in the future, the Court had to balance governmental interests with citizens' privacy and technological advances that make private information all the more accessible to the public at large.

A. Background

At issue in *Doe v. Reed* was the combination of Washington's laws concerning petitions and referendums and its Public Records Act. Washington is one of the twenty-four states that permits its citizens to change legislation through the referendum process.[43] If enough signatures are gathered in a petition, a referendum will be added to the general election ballot to allow the voters to decide whether to repeal legislation.[44] A person signing a petition is required to put his or her legal name, address, and signature.[45] When the state determines if there are sufficient signatures to include a measure on the ballot, Washington law permits observers from both those that support and oppose a measure to be present to observe the state's verification process "so long as they make no record of the names, addresses, or other information on the petitions or related records. . . ."[46] Aside from the observer provision, Washington law is silent concerning whether the names or other information on a petition are public documents.

Washington's Public Records Act ("PRA") requires each state agency to make available for public inspection and copying "all public records," unless those

records fall within certain exemptions.[47] The PRA was passed with the express intent that Washington citizens remain "informed so that they may maintain control over the instruments that they have created."[48] In the context of campaign finance disclosures, the policy of disclosure is further espoused by the state of Washington: "mindful of the right of individuals to privacy and of the desirability of the efficient administration of government, full access to information concerning the conduct of government on every level must be assured as a fundamental and necessary precondition to the sound governance of a free society."[49]

In 2009, Washington's legislature enacted a law to expand the state's existing domestic partnership law to provide registered domestic partners virtually all the state-law rights of married couples.[50] The law was referred to as the "everything but marriage bill."[51] Citizens who opposed same-sex marriage wanted to repeal the law and turned to Washington's referendum process. The newly formed "Protect Marriage Washington" group organized to collect a sufficient number of signatures on a petition and submitted it to the state for final approval.[52]

Supporters of the partnership law requested copies of the petition under Washington's PRA.[53] Although not part of the regulations governing petitions and referendums, Washington's PRA permitted public access to a wide range of documents in the possession of the state.[54] For years, state officials had taken the position that the names on petitions were not considered public records and thus, were not made publicly available.[55] Sam Reed, the current Secretary of State for Washington, considered the petitions to be public records and as a result, subject to the public records law.[56] Some groups in support of the partnership law issued press releases that they would make the names of petition signers available on the Internet and in a searchable format.[57]

This was all developing in Washington against the backdrop of the debate in California over Proposition 8. Petition signers in Washington were concerned that the public availability of their identities could lead to harassment and intimidation, as it appeared to have done so with respect to the Proposition 8 supporters in California who contributed money to the cause.[58] Two signers of the petition filed suit as anonymous John Does arguing the Washington disclosure laws were unconstitutional under both a facial and an as-applied theory: (1) the disclosure of petition signers names was unconstitutional because it would deter people from signing petitions; and (2) even if the disclosure law passes constitutional muster generally, these plaintiffs were entitled to an exception to the disclosure requirement because the law was unconstitutional as-applied to their particular circumstances.[59] The petition signers asked the court to preliminarily enjoin the Secretary of State from releasing the petition names.[60]

B. Lower Court Decisions

The U.S. District Court for the Western District of Washington granted the petition signers' motion for a preliminary injunction on the basis that they were likely to succeed on their facial

challenge and enjoined the release of the petitions.[61] Upon review, the Court of Appeals for the Ninth Circuit reversed the injunction.[62] On appeal to the U.S. Supreme Court, the petition signers convinced the Court to stay the Ninth Circuit ruling, so the petitions would not be released prior to the election.[63] The referendum was ultimately defeated and the state's domestic partnership law is now in effect.[64]

C. Amicus Briefs

Given the backdrop of the gay-marriage issue, the case garnered media interest and the attention of many organizations, who then filed amicus briefs. Fifteen amicus briefs were filed in support of the signers of the petition, [65] and ten were filed in support of the State of Washington[66]. States with similar disclosures laws filed an amicus brief emphasizing the government's interest in making petitions publicly available.[67] Some organizations discussed how the existence of the Internet has drastically enhanced the ability for anyone to learn a great deal of information about an individual.[68] These organizations argued that if petition signers' names and addresses are easily found in the Internet, it may be more difficult to convince people to sign petitions.[69] Other groups cited examples from around the world where those who sign petitions face threats and retribution.[70] They argued that the petition signers should not be subject to such risks when Washington's referendum law already allows for certain public oversight to prevent fraud.[71] In their view, much less intrusive means already exist to protect the electoral process than making the petition names subject to general disclosure laws.[72]

D. U.S. Supreme Court Decision

The U.S. Supreme Court held, 8-1, that the First Amendment does not categorically ban public access to the names and addresses of supporters of state-wide initiatives and referendums.[73] The Court determined that First Amendment challenges in the electoral context required the "exacting scrutiny" test where "the strength of the governmental interest must reflect the seriousness of the actual burden on the First Amendment rights."[74] As discussed in more detail below, the Court left for another day whether the privacy of signers might outweigh the public interest in disclosure if the signers could prove specific harm from disclosure.

1. The Majority Opinion

Chief Justice Roberts, joined by Justices Kennedy, Ginsburg, Breyer, Alito and Sotomayor, wrote for the majority and as an initial matter, found that the First Amendment applied because "[a]n individual expresses a view on a political matter when he signs a petition. . . ."[75] On the other side of the scale, the majority acknowledged that States are given "significant flexibility in implementing their own voting systems."[76] The petition signers had argued that the Court should apply the strict scrutiny test. In explaining why disclosure requirements were subject to the less demanding "exacting scrutiny," rather than "strict scrutiny," the Court emphasized that the statute at issue was

"not a prohibition on speech, but instead a ***disclosure*** requirement."[77] In *Citizens United*, the campaign finance case decided earlier that same term, the Court noted that "disclosure requirements may burden the ability to speak, but they 'impose no ceiling on campaign-related activities' and 'do not prevent anyone from speaking.'"[78] The *Reed* Court relied on a long history of First Amendment cases in the electoral context to provide the "exacting scrutiny" standard.[79] This standard "requires a substantial relation between the disclosure requirement and a sufficiently important governmental interest."[80] Moreover, "[t]o withstand this scrutiny, the strength of the government interest must reflect the seriousness of the actual burden on First Amendment rights."[81]

Washington had argued that its interests included "(1) preserving the integrity of the electoral process by combating fraud, detecting invalid signatures, and fostering government transparency and accountability; and (2) providing information to the electorate about who supports the petition."[82] The Court found the first reason sufficiently compelling that it did not address the second reason.[83] The majority opinion explained:

> The State's interest is particularly strong with respect to efforts to root out fraud, which not only may produce fraudulent outcomes, but has a systemic effect as well: It "drives honest citizens out of the democratic process and breeds distrust of our government."[84]

Washington and other states filing amici briefs cited to several cases of petition-related fraud.[85] Even short of fraud, the Court noted that the state has an interest in allowing the petition signers' identities to be public to preserve the integrity of the electoral process in general.[86] Although the government might be positioned to combat fraud without disclosing the petition signers' names, the Court noted that citizens themselves are in the best position to uncover other types of problems in the petition process: "Public disclosure also promotes transparency and accountability in the electoral process to an extent other measures cannot."[87] Thus, the majority held that the public disclosure laws were substantially related to the government interest in preserving the integrity of the electoral process.

The majority opinion left open the possibility that the petitioners could continue their legal challenge on an "as applied" basis. The Court noted that "upholding the [disclosure] law against a broad-based challenge does not foreclose a litigant's success in a narrower one."[88] The Court cited to what it considered the relevant standard petitioners will have to satisfy on the as-applied challenge—the disclosure may be unconstitutional if the petitioners can show "a reasonable probability that the compelled disclosure of personal information will subject them to threats, harassment, or reprisals from either Government officials or private parties."[89] The petition signers' fight now continues in the lower courts.[90]

2. Concurring Opinions

While the decision at first glance appears to be an easy one—8-1—there were no less than six separate opinions in the majority. Five justices joined Chief Justice Robert's majority opinion. Justice Alito and Justice Breyer filed concurring opinions. Justice Sotomayor filed a concurring opinion joined by Justice Stevens and Justice Ginsburg. Justice Stevens filed an opinion concurring in part and concurring in the judgment, in which Justice Breyer joined. Justice Scalia joined in the judgment only and wrote a separate concurring opinion.

The concurring opinions of Justice Scalia, Justice Sotomayer, and Justice Alito represent three very different approaches to balancing the privacy interests of the petition signers with the government's interest in regulating elections. Justice Scalia regards the act of signing a petition much like a legislative act and as a result, void of any expectation of privacy. In stark contrast, Justice Alito sees the act of signing a petition as an act protected by the First Amendment right to the privacy of association and belief. While agreeing with the majority to uphold the disclosure laws on a facial challenge, Justice Alito is sympathetic to the petition signers' as-applied challenge and thinks their burden of proof should be low. Justice Sotomayor's concurrence explores the middle ground between those two extremes. Her opinion recognizes the First Amendment protection for the expressive nature of signing a petition, but sets a high hurdle for the petition signers to clear in order to prevail on their as-applied challenge.

i. Justice Scalia Concurrence

Although Justice Scalia joined in the judgment upholding Washington's disclosure laws, his opinion is very different from the majority. Justice Scalia doubts whether the First Amendment even applies to the act of signing a petition because he views it as a legislative act.[91] Justice Scalia repeats much of the analysis from his dissent in the *McIntyre v. Ohio Elections Commission* case, the case in which the court recognized the First Amendment rights to distribute anonymous campaign literature.[92] Justice Scalia takes the position that there is no First Amendment right to anonymity.[93] He cites to this country's "longstanding traditions of legislating and voting in public" to refute the claim that the First Amendment protects anonymity in the performance of an act with "governmental effect."[94] "[T]he exercise of lawmaking power in the United States has traditionally been public."[95] Scalia also explains that voting was historically a public act as well and that the Court has never recognized a right to vote anonymously.[96]

Justice Scalia is skeptical of the petition signers' ability to prove an as-applied challenge that would exempt them from disclosure laws. He states that "[r]equiring people to stand up in public for their political acts fosters civic courage, without which democracy is doomed."[97] He laments a society that allows anonymous campaigns where direct democracy is "hidden from public scrutiny and protected from the accountability of criticism."[98] And in what might be the most quoted language from his opinion, Scalia remarks: "This

does not resemble the Home of the Brave."[99]

ii. Justice Alito Concurrence

Justice Alito's concurrence reads more like a dissent because he goes into great detail about the strength of the petition signers' case for their as-applied challenge. Alito agrees with the majority that the disclosure requirements survive a facial challenge, but believes the petition signers have a strong as-applied case in that the disclosure laws can "seriously infringe on privacy of association and belief guaranteed by the First Amendment."[100] In contrast to Justice Scalia, Justice Alito's concurrence is concerned with the burdens placed on the petition signers' freedom of speech and association and privacy rights.[101]

Justice Alito makes an important caveat in his concurrence. While he believes the as-applied challenge is the proper route for the petition signers to seek exemption from the disclosure laws, he notes that their First Amendment rights will be adequately protected only if "(1) speakers can obtain the exemption sufficiently far in advance to avoid chilling protected speech and (2) the showing necessary to obtain the exemption is not overly burdensome."[102] If these requirements are not met, then Justice Alito is concerned that the disclosure laws might have a chilling effect on voters' willingness to sign petitions because of the uncertainty of whether their information will be disclosed.[103] Consequently, he advocates that as-applied challenges must take place before a voter is asked to sign the petition so the signer will know at the time of signing whether their name will be public.[104]

Justice Alito then outlines the strengths he sees in the petition signers' as-applied challenge that outweighs the state's interests. Justice Alito is especially critical of the state's "informational interest."[105] Washington had argued that the disclosure of petition signers names provided the public with insight into whether support for a measure comes from a particular group of citizens and that this information then assists a voter in deciding whether to support or oppose the measure.[106] Justice Alito notes that simply providing the public with the names and addresses of petition signers does not give the public the type of information that the state says voters need to decide whether to oppose or support a measure.[107] The state's informational interest implies that the state would have an interest in gathering and disclosing other sensitive information like race, religion and sexual orientation.[108] Obviously the public release of that information runs head-on into firmly established rights of privacy.[109]

Justice Alito is also critical of the state's interest in preserving the integrity of the electoral process. He points out that the petition process already provides for observers to view the government's review of petition signatures for validity.[110] Justice Alito also explains that Washington has only recently taken the position that petition signatures are subject to state disclosure laws.[111] Previously, the state did not release that information and Justice Alito claims the state has not justified how circumstances have changed to now necessitate the public disclosure of the petition signers'

names.[112] Justice Alito cites to California as the example of a state that keeps petitions signers' names private and maintains a process free from fraud.[113] Finally, Justice Alito suggests several ways the state of Washington could "easily and cheaply employ alternative mechanisms for protecting against fraud and mistake that would be far more protective of circulator's and signer's First Amendment rights."[114]

Justice Alito sees the as-applied challenges as "critical" in protecting First Amendment Freedoms: "To give speech the breathing room it needs to flourish, prompt judicial remedies must be available well before relevant speech occurs and the burden of proof must be low."[115] He concludes that the petition signers in *Doe v. Reed* have a "strong case" that they are entitled to relief.[116]

iii. Justice Sotomayor Concurrence

Justice Sotomayor's concurrence, joined by Justice Stevens and Justice Ginsburg, recognizes the expressive interest in signing a petition, but wastes no time noting that disclosure does not impair the expressive nature of that act or the associational rights of the signers.[117] Her opinion emphasizes the "considerable leeway" states are given to decide what issues are placed on the ballot and to set forth the procedure for ballot access.[118] Her opinion strongly favors disclosure laws, explaining that the referendum process is "inherently public," with citizens signing in public with no guarantee of confidentiality.[119] In this way, she rejects the idea that signing a petition is akin to casting a secret ballot.[120]

In contrast to Justice Alito, Justice Sotomayor gives significant weight to the interest of the states to manage their electoral processes and thus, her opinion is critical of the as-applied challenge.[121] She explains that petition signers will bear a "heavy burden" to prove the "rare circumstance in which disclosure poses a reasonable probability of serious and widespread harassment that the State is unwilling or unable to control."[122] She concludes with this guidance for the courts below:

> [C]ourts presented with an as-applied challenge to a regulation authorizing disclosure of referendum petitions should be deeply skeptical of any assertion that the Constitution, which embraces political transparency, compels States to conceal the identity of persons who seek to participate in lawmaking through a state-created referendum process.[123]

3. Justice Thomas Dissent

Given Justice Thomas's partial dissent in *Citizen's United* earlier in the term, where he discussed the harassment faced by the proponents of Proposition 8 in California, his dissent in this case was not a surprise.[124] Indeed, Justice Thomas is the most vocal advocate of protecting the petition signers' privacy. He would have struck down Washington's application of the disclosure laws to the referendum process because he finds "there will always be a less restrictive means by which Washington can vindicate its stated interest in preserving

the integrity of its referendum process."[125]

Justice Thomas's biggest divergence from the majority is his application of the *NAACP v. Alabama* line of cases. He determines that strict scrutiny should apply because signing a referendum amounts to political association.[126] Justice Thomas explains the many things Washington could do to further its interest in preserving the integrity of the electoral process, without burdening petition signers' First Amendment rights.[127] For example, Washington could institute an electronic referendum database.[128] Justice Thomas explains that the state's informational interest is in contravention of the Court's protection of anonymous political speech in *McIntyre v. Ohio Elections Commission*.[129] For these reasons, Justice Thomas would hold that the disclosure laws are not narrowly tailored to apply to any referendum and would grant the facial challenge.[130]

Justice Thomas concludes by describing the "[s]ignificant practical problems" that will result from requiring petition signers to use as-applied challenges, in particular, the chilling of protecting speech.[131] Justice Thomas explicitly addresses the changes in technology and their impact on privacy rights:

> [T]he state of technology today creates at least *some* probability that singers of every referendum will be subjected to threats, harassment, or reprisals if their personal information is disclosed. The advent of the Internet enables rapid dissemination of the information needed to threaten or harass every referendum signer. Thus, disclosure permits citizens to react to the speech of their political opponents in a proper—or undeniably *improper*—way long before a plaintiff could prevail on an as-applied challenge.[132]

Justice Thomas concludes that the problem with ever being able to bring a timely challenge to the disclosure laws means that not only are the First Amendment rights of petition signers harmed, but the direct democracy process as a whole will be harmed:

> This chill in protected First Amendment activity harms others besides the dissuaded signer. We have already expressed deep skepticism about restrictions that make it less likely that a referendum will garner the number of signatures necessary to place the matter on the ballot, thus limiting the ability to make the matter the focus of statewide discussion. Such restrictions inevitably reduce the total quantum of speech on a public issue. The very public that the [Washington disclosure law] is supposed to serve is thus harmed by the way Washington implements that statute here.[133]

IV. Future Implications of *Doe v. Reed*

While the majority opinion in *Doe v. Reed* did not address the as-applied challenge to Washington's disclosure law, the concurring and dissenting opinions did not shy away from providing specific guidance to the lower courts. The

majority decision in dicta referred to the standard for minor political parties to obtain an exemption from a disclosure law from *Buckley v. Valeo*: that the disclosure may be unconstitutional as applied to petition signers if they can show "a reasonable probability that the compelled disclosure of personal information will subject them to threats, harassment, or reprisals from either Government officials or private parties."[134] The court was deeply divided over the showing that might be sufficient to support an exception to the disclosure requirement. Justice Alito argued that the as-applied challenge should be easy.[135] In contrast, Justice Scalia argued that the as-applied challenge, if allowed at all, should make it exceptionally difficult to prove.[136] The chances the specific petition signers in *Doe v. Reed* will prevail is unlikely, given that five members of the Court (Justice Stevens, Justice Breyer, Justice Sotomayor, Justice Ginsburg, and Justice Scalia) either expressed significant doubts or outright rejected the likelihood of the as-applied challenge succeeding.[137] With Justice Stevens' retirement this past year, petition signers may think they have a chance to sway Justice Stevens' replacement, Justice Elaina Kagan. Justice Alito and Justice Thomas are sympathetic to the petition signers and would likely grant their as-applied challenge. Justice Roberts and Justice Kennedy signed the majority opinion in *Doe v. Reed*, but did not sign onto any of the concurrences, so their respective positions on the as-applied challenges are likely somewhere in the middle.

Ultimately, to prevail on an as-applied challenge to a disclosure law, privacy proponents will need to be creative in convincing the courts that they are reasonably likely to be subjected to threats, harassment, or reprisals if their private information is made public. The Supreme Court has held that sufficient proof includes "specific evidence of past or present harassment of members due to their associational ties, or of harassment directed against the organization itself. A pattern of threats or specific manifestations of public hostility may be sufficient. New parties that have no history upon which to draw may be able to offer evidence of reprisals and threats directed against individuals or organizations holding similar views."[138] Historically, groups have succeeded in as-applied challenges by presenting evidence of threatening phone calls and hate mail towards their members, as well as harassment by employers, the police, and the government itself.[139] It remains to be seen whether more modern forms of "harassment," such as online "bullying," standing alone, will be sufficient to obtain an exemption from disclosure laws. Certainly, in the Digital Age, it has become easier for politically motivated groups to attempt to threaten or intimidate their opponents through email, social media websites, blogs, and sites such as eightmaps.com. This type of harassment might well be enough to dissuade would-be petition signers from signing on to a petition that they support. But, is this enough to overcome the state's interests in regulating its election process, informing the electorate, and detecting fraud in the petition process? This is a balancing act that courts will be forced to grapple with in addressing as-applied challenges.

Interestingly, the Court in *Doe v. Reed*, albeit in *dicta*, seemingly expanded the somewhat lenient standard for exemption to disclosure for minor political parties to *any* group resisting disclosure.[140] Originally, the rationale for allowing minor political parties "flexibility in the proof of injury" was that minor political parties were more vulnerable and less likely to influence an election. As the Court stated in *Buckley v. Valeo:*

> It is true that the governmental interest in disclosure is diminished when the contribution in question is made to a minor party with little chance of winning an election. As minor parties usually represent definite and publicized viewpoints, there may be less need to inform the voters of the interests that specific candidates represent. Major parties encompass candidates of greater diversity. . . . The Government's interest in deterring the "buying" of elections and the undue influence of large contributors on officeholders also may be reduced where contributions to a minor party or an independent candidate are concerned, for it is less likely that the candidate will be victorious. . . . We are not unmindful that the damage done by disclosure to the associational interests of the minor parties and their members and to supporters of independents could be significant. These movements are less likely to have a sound financial base and thus are more vulnerable to falloffs in contributions. In some instances fears of reprisal may deter contributions to the point where the movement cannot survive. The public interest also suffers if that result comes to pass, for there is a consequent reduction in the free circulation of ideas both within and without the political arena.[141]

Before *Doe v. Reed*, it was debatable whether *Buckley*'s lenient standard for obtaining an as-applied challenge should apply to any group who fears reprisal from political opponents, or only to minor parties. On the one hand, the government has a more compelling case for enforcing its disclosure laws with respect to political groups who are in the majority. As the Supreme Court opinions have noted, compelled disclosure laws help to inform the electorate, which promotes valuable First Amendment principles and foster civic engagement. On the other hand, and especially with the potential for widespread dissemination of information in the Digital Age, majority groups may be just as susceptible to threats and harassment for their political views as minority parties. For example, the "Protect Marriage" groups claim that, although their opposition to gay marriage currently represents the viewpoint of the majority of Americans,[142] they are susceptible to harassment from gay rights minority groups. Admittedly, majority groups are unlikely to face the systemic types of reprisal that the minority groups such as the NAACP or the Socialist party faced throughout the last century, such as loss of employment and government surveillance. But at the end of the day, are the privacy interests of members of majority groups any less important? Moreover, the distinction between

minority and majority groups becomes hard to discern when it comes to initiatives and referendums. As the Supreme Court noted in *Doe v. Reed*, petition signers may simply sign to show support for the notion that an issue should be decided by the people, rather than to show support of the initiative or referendum itself. It may also be difficult to determine whether supporters of an initiative or referendum represent the majority or minority position. Oftentimes, this will not be known until after the initiative or referendum is voted upon. Even then, a position may be in the minority in one community and in the majority in another. Should the courts examine the likelihood of harassment or reprisal on a local level, a state level, or a national level? These are only some of the interesting questions that will have to be addressed as the lower courts grapple with the standard the U.S. Supreme Court suggests in *Doe v. Reed*.

While lower courts might struggle with the application of *Doe v. Reed* to as-applied challenges, much of this debate may be left in the hands of the states themselves, where several Justices in *Doe v. Reed* implied it belongs.[143] Although the petition signers in *Doe v. Reed* lost their facial challenge and will likely face an uphill battle for their as-applied challenge, they could seek more privacy protections by changing state disclosure laws. Several Justices noted the deference the Court gives to states to regulate their own electoral process.[144] If it appears the technological advancements that make public release of information like petition signatures are chilling that particular form of direct democracy, states could legislate an exception to their government record laws and keep private the names of petition signers. States could also modify their state constitutions to provide privacy protections to petition signers beyond the protections in the federal constitution. Justice Scalia noted in his concurring opinion that although there is no constitutional right to an anonymous ballot, many states took measures to ensure a secret ballot.[145] Scalia explains that if states are concerned about the threats and intimidation that might result from public disclosure of petition signatures, they can change their laws to keep the signatures from the scope of disclosure laws.[146] States could also guard against fraud in some of the ways Justice Alito and Thomas suggested, thereby decreasing the need for the petition signers' names to be public.[147] California currently is the only state with a petition process that exempts petition signers from public disclosure.[148] Interestingly, a measure was recently introduced in the Washington state legislature that would have excluded petition signatures from public disclosure, but it failed to pass.[149] In true "direct democracy" fashion, voters could petition to include a measure on the ballot that would exclude petitioners' names from public disclosure.

The inherent tension between privacy rights and public disclosure laws will continue to be played out in the lower courts and at the state level. In this way, *Doe v. Reed* raises many more questions than it settled and we are likely to see the as-applied challenges back before the Court in the near future.

[1] *State-by-State List of Initiative and Referendum Provisions*, INITIATIVE AND REFERENDUM INST., http://www.iandrinstitute.org/statewide_i%26r.htm (last visited Dec. 11, 2010); *Chart of Initiative and Referendum States*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=16589 (last visited Dec. 11, 2010). For an overview of the different types of initiatives, *see* Initiative and Referendum Institute, www.iandrinstitute.org.

[2] INITIATIVE AND REFERENDUM INST., *supra* note 1; NAT'L CONFERENCE OF STATE LEGISLATURES, *supra* note 1.

[3] *Ballot Initiative Strategy Center State by State Report Card*, BALLOT INITIATIVE STRATEGY CTR. (July 2009), http://bisc.3cdn.net/1fb0aa12d865ddd8c6_wwm6b9zwc.pdf; CAL. GOV'T CODE §§ 6253.5, 6253.6 (Deering 2010).

[4] *A Brief History of the Initiative and Referendum Process in the United States*, INITIATIVE AND REFERENDUM INST., http://www.iandrinstitute.org/New%20IRI%20Website%20Info/Drop%20Down%20Boxes/Quick%20Facts/History%20of%20I&R.pdf (last visited Dec. 11, 2010); David B. Magleby, *Governing by Initiative: Let the Voters Decide? An Assessment of the Initiative and Referendum Process*, 66 U. COLO. L. REV. 13, 14-15 (1995).

[5] INITIATIVE AND REFERENDUM INST., *supra* note 4.

[6] *I&R Historical Timeline*, INITIATIVE AND REFERENDUM INST., http://www.iandrinstitute.org/New%20IRI%20Website%20Info/Drop%20Down%20Boxes/Quick%20Facts/Almanac%20-%20I&R%20Historical%20Timeline.pdf (last visited Dec. 11, 2010).

[7] INITIATIVE AND REFERENDUM INST., *supra* note 4.

[8] INITIATIVE AND REFERENDUM INST., *supra* note 4.

[9] *Initiative Use*, INITIATIVE AND REFERENDUM INST. (Sept. 2010), http://www.iandrinstitute.org/IRI%20Initiative%20Use%20(2010-1).pdf.

[10] INITIATIVE AND REFERENDUM INST., *supra* note 9.

[11] INITIATIVE AND REFERENDUM INST., *supra* note 9; *Ballotwatch*, INITIATIVE AND REFERENDUM INST. (Nov. 2010), http://www.iandrinstitute.org/BW%202010-2%20Election%20Results%20(11-6).pdf.

[12] *See* Burson v. Freeman, 504 U.S. 191, 203 (1992) (plurality opinion).

[13] *Id.*

[14] U.S. CONST. Amend. I. ("Congress shall make no law … abridging … the right of the people peaceably to assemble."); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 995 (2003).

[15] 357 U.S. 449, 462 (1958).

[16] *Id.* at 466.

[17] *Id.* at 462-63.

[18] By the same token, it is also argued that privacy protections which protect against the disclosure of true information conflict with the First Amendment's guarantee of freedom of speech. *See, e.g.*, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1090, 1095 (2000).

[19] 424 U.S. 1, 64 (1976).

[20] 459 U.S. 87, 91 (1982).

[21] 514 U.S. 334, 342-43 (1994).

[22] Buckley v. Valeo, 424 U.S. at 64.

[23] *Id.*; *see also* NAACP v. Alabama, 357 U.S. 449, 462-63 (1958).

[24] *McIntyre*, 514 U.S. at 357.

[25] Buckley v. ACLF, 525 U.S. 182, 200 (1999).

[26] Buckley v. Valeo, 424 U.S. at 84.

[27] *Id.* at 66-68.

[28] 514 U.S. at 348.

[29] *Id.* at 348 n.11.

[30] *Id.* at 349.

[31] Buckley v. ACLF, 525 U.S. 182, 198-99 (1999).

[32] Buckley v. Valeo, 424 U.S. at 70-71.

[33] *Id.* at 74.

[34] HUFFPOST FUNDRACE, http://fundrace.huffingtonpost.com/ (last visited Dec. 13, 2010).
[35] *Id.*
[36] *See, e.g.*, CANIVOTE.ORG, http://www.canivote.org/ (last visited Dec. 13, 2010) (providing links to states' websites).
[37] *See, e.g.*, GOTVOTERS ONLINE, http://www.voter-lists.com/voter-lists.cfm (last visited Dec. 13, 2010).
[38] Brad Stone, *Prop 8 Donor Web Site Shows Disclosure Law Is 2-Edged Sword*, N.Y. TIMES, Feb. 7, 2009, www.nytimes.com/2009/02/08/business/08stream.html.
[39] PROP 8 MAPS, http://www.eightmaps.com (last visited Dec. 13, 2010).
[40] Stone, *supra* note 38 ("'When I see those maps, it does leave me with a bit of a sick feeling in my stomach,' said Kim Alexander, president of the California Voter Foundation, which has advocated for open democracy. 'This is not really the intention of voter disclosure laws. But that's the thing about technology. You don't really know where it is going to take you.'").
[41] Stone, *supra* note 38.
[42] Stone, *supra* note 38.
[43] WASH. CONST., art. II, §1(b), (d); WASH REV. CODE §§ 29A.72.010—.290 (2010).
[44] In the case of a referendum, the "person or organization demanding any referendum of an act or part of an act of the legislature has obtained a number of signatures of legal voters equal to or exceeding four percent of the votes cast for the office of governor at the last regular gubernatorial election prior to the submission of the signatures for verification. . . ." § 29A.72.150.
[45] § 29A.72.130.
[46] § 29A.72.230.
[47] § 42.56.070(1).
[48] § 42.56.030 .
[49] § 42.17.010(11).
[50] S.B. 5688, 61st Leg., Reg. Sess. (Wash. 2009).
[51] *See* Rachel La Corte, *Lawmakers Announce 'Everything But Marriage' Bill*, SEATTLE TIMES, Jan. 28, 2009, http://seattletimes.nwsource.com/html/localnews/2008678540_apwaxgrdomesticpartnerships2ndldwritethru.html; Lornet Turnbull, *Gregoire Expands Same-Sex Partnerships*, SEATTLE TIMES, May 18, 2009, http://seattletimes.nwsource.com/html/localnews/2009233610_webdomestic18.html.
[52] *See* Doe v. Reed, 130 S.Ct. 2811, 2816 (2010).
[53] *Id.*
[54] *See, e.g.*, § 42.56.070
[55] *See, e.g.*, Wash. Op. Att'y Gen. 55-57 No. 274 (1956).
[56] Brief for Respondents at 5-6, Doe v. Reed, 130 S.Ct. 2811 (2010) (No. 09-559).
[57] Press Release, KnowThyNeighbor.org, Whosigned.org Refutes Intimidation Charges; Will Post Names of Petition Signers as Planned (June 8, 2009), http://knowthyneighbor.blogs.com/home/2009/06/whosignedorg-refutes-intimidation-charges-will-post-names-of-petition-signers-as-planned.html ("While he acknowledges that some find it surprising to learn that petition information is a matter of public record, [Aaron] Toleos [co-director of KnowThyNeighbor.org] says, 'Anyone that is honest about wanting a clean, transparent process should welcome the scrutiny that our website makes possible. And if they don't, you should wonder why.'").
[58] Brief for Petitioners at 10, *Doe v. Reed*, 130 S.Ct. 2811 (2010) (No. 09-559).
[59] *See* Doe v. Reed, 130 S.Ct. 2811, 2816 (2010).
[60] *Id.*
[61] Doe v. Reed, 661 F. Supp.2d 1194, 1205-06 (W.D. Wash. 2009).
[62] Doe v. Reed, 586 F.3d 671, 681 (9th Cir. 2009).
[63] *See* Adam Liptak, *Court to Rule on Right to Privacy for Referendum Petition Signers*, N.Y. TIMES, Jan. 16, 2010, at A13.
[64] *Id.*
[65] The briefs in support of the petitioners included those filed by the following groups: Common Sense for Oregon, the Oregon Anti-

Crime Alliance, and Oregonians in Action; Concerned Women for America; Institute for Justice; CATO Institute; American Center for Law and Justice; American Civil Rights Union; Committee for Truth in Politics, the National Organization for Marriage, the Family Research Council, and American Values; Voters Want More Choices; Alliance Defense Fund; Protectmarriage.com-Yes on 8, A Project of California Renewal; Liberty Counsel; The Abraham Lincoln Foundation for Public Policy Research, Inc., American Conservative Union, American Target Advertising, Inc., Citizens in Charge Foundation, Citizens United, Citizens United Foundation, ClearWord Communications Group, Inc., the Conservative Legal Defense and Education Fund, The Constitution party National Committee, Downsize DC Foundation, SownsizeDC.org, Eberle & Associates, Inc., English First, English First Foundation, Free Speech Coalition, Inc., The Free Speech Defense And Education Fund, Inc., Gun Owners Foundation Gun Owners of America, Inc., the Institute on the Constitution, law Enforcement Alliance of America, Inc., The Lincoln Institute for Research and Education, the National Right to Work Legal Defense and Education Foundation, Inc., Production Solutions, Inc. Public Advocate of the United States, The Richard Norman Company, 60 Plus Association, U.S. Border Control, U.S. Border Control Foundation, U.S. Justice Foundation, and Young America's Foundation; and Center for Constitutional Jurisprudence.

[66] The briefs in support of the respondents included those filed by the following groups: Direct Democracy Scholars; City of Seattle; National and Washington State News Publishers, News Broadcasters and News Media Professional Associations; States of Ohio, Arizona, Colorado, Florida, Idaho, Illinois, Maine, Maryland, Massachusetts, Mississippi, Montana, New Hampshire, New Jersey, New Mexico, North Dakota, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Utah, Vermont, and Wisconsin; Lambda Legal Defense and Education Fund, Inc., Gay & Lesbian Advocates & Defenders, National Center for Lesbian Rights, the Human Rights Campaign, and National Gay and Lesbian Task Force; Reporters Committee for Freedom of the Press, Gannett Co., Inc., National Newspaper Association, Newspaper Association of America, The Radio-Television Digital News Association, and Society of Professional Journalists; National Conference of State Legislatures, International City/County Management Association, National Association of Countries, and International Municipal Lawyers Association; American Business Media, Consumer Data Industry Association, First American Corelogic, Inc., the National Association of Professional Background Screeners, Reed Elsevier, Inc., the Software & Information Industry Association, Transunion, and Thomson Reuters; National Conference of State Legislatures, the International City-County Management Association, the National Association of Counties, and the International Municipal Lawyers Association; and Massachusetts Gay and Lesbian Political Caucus and Susan Wagner.

[67] Brief for States of Ohio, Arizona, Colorado, Florida, Idaho, Illinois, Maine, Maryland, Massachusetts, Mississippi, Montana, New Hampshire, New Jersey, New Mexico, North Dakota, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Utah, Vermont, and Wisconsin in Support of Respondents, Doe v. Reed, 130 S.Ct. 2811 (2010) (No. 09-559).

[68] *See, e.g.*, Brief for Committee for Truth in Politics, National Organization for Marriage, Family Research Council, and American Values as Amici Curiae in Support of Petitioners at 8-17, Doe v. Reed, 130 S.Ct. 2811 (2010) (No. 09-559).

[69] *Id.* at 21-25.

[70] Brief for Electronic Privacy Information Center (EPIC) and Legal Scholars and Technical Experts as Amici Curiae in Support

of Petitioners at 15-19, Doe v. Reed, 130 S.Ct. 2811 (2010) (No. 09-559).
[71] *Id.* at 23-29.
[72] *Id*.
[73] Doe v. Reed, 130 S.Ct. 2811 (2010).
[74] *Id*. at 2814.
[75] *Id*. at 2817.
[76] *Id*. at 2818.
[77] *Id*.
[78] Citizens United v. FEC, 130 S. Ct. 876, 914 (2010) (quoting Buckley v. Valeo, 424 U.S. 1, 64 (1976); McConnell V. FEC, 540 U.S. 93, 201 (2003)).
[79] *Reed*, 130 S.Ct. at 2818. This line of cases goes all the way back to *Buckley*, 424 U.S. 1 through *Citizens United*, 130 S.Ct. 876.
[80] *Reed*, 130 S.Ct. at 2818. In this sense, Reed confirmed that "exacting scrutiny" will be the standard that applies in disclosure campaign finance cases as well. Lower courts have already cited to *Reed* for that proposition. *See* Human Life of Wash., Inc. v. Brumsickle, No. 09-35128, 2010 U.S. App. LEXIS 21028 at *34 (9th Cir. Oct. 12, 2010) ("As the latest in a trilogy of recent Supreme Court cases, *Reed* confirmed that exacting scrutiny applies in the campaign finance disclosure context. We therefore apply exacting scrutiny to Human Life's facial challenges to the Disclosure Law and examine whether the law's requirements are substantially related to a sufficiently important governmental interest.").
[81] *Reed*, 130 S.Ct. at 2818.
[82] *Id*. at 2819.
[83] *Id.*
[84] *Id*.
[85] *Id.*
[86] *Id.* at 2820.
[87] *Id*..
[88] *Id*. at 2821.
[89] *Id*. at 2820 (citing *Buckley*, 424 at 74; *Citizens United*, 130 S.Ct. 876).
[90] *See* Janet I. Tu & Kyung M. Song, *Ref. 71 Signatures are Public, Supreme Court Rules*, SEATTLE TIMES, June 24, 2010, http://seattletimes.nwsource.com/html/localnews/2012196559_scotus25m.html.
[91] *Id*. at 2833 (Scalia, J., concurring).
[92] *Id*. at 2832.
[93] *Id*.
[94] *Id*. at 2832-33.
[95] *Id*. at 2833.
[96] *Id*. at 2834-35.
[97] *Id*. at 2837.
[98] *Id*.
[99] *Id*.
[100] *Id*. at 2822 (Alito, J., concurring).
[101] *Id*. at 2822-23.
[102] *Id*. at 2822.
[103] *Id*. at 2822-23.
[104] *Id*.
[105] *Id*. at 2824.
[106] *Id.*
[107] *Id*.
[108] *Id*.
[109] *Id*.
[110] *Id*. at 2825-26.
[111] *Id*. at 2826.
[112] *Id*.
[113] *Id*. at 2826-27.
[114] *Id*. at 2827.
[115] *Id*.
[116] *Id*.
[117] *Id*. at 2828-29 (Sotomayor, J., concurring).
[118] *Id*. at 2827.
[119] *Id*. at 2828.
[120] The distinction between whether signing a petition is more like a legislative act or like casting secret ballot has been debated by various courts. For example, in Shepherdstown Observer, Inc. v. Maghan, No. 35446, 2010 W. Va. LEXIS 98 (W. Va. Sept. 23, 2010), the West Virginia Supreme Court of Appeals consider the ruling of a lower state court that dismissed a complaint seeking the names of those that signed petitions, at least partially, on the grounds that petition signers had privacy interests in signing a petition because it was similar to casting a secret ballot. *Id.* at *21-22. The court reversed, citing to Doe v. Reed, and held that the lower court had erred in finding the signing of a petition as the functional equivalent to casting a secret ballot. *Id*. at **27-30. Just as in *Doe*

v. Reed, the *Shepherdstown* court found that the state's interest in protecting the integrity of the electoral process outweighed any First Amendment interests of the petition signers. *Id*. at *30.

[121] *Reed*, 130 S.Ct. at 2828-29 (Sotomayor, J., concurring).

[122] *Id*. at 2829.

[123] *Id*.

[124] *See* Citizens United v. FEC, 130 S.Ct. 876, 980 (2010) (Thomas, J., dissenting).

[125] *Reed*, 130 S.Ct. at 2838 (Thomas, J., dissenting).

[126] *Id*. at 2839.

[127] *Id*. at 2841.

[128] *Id*.

[129] *Id*. at 2842-43.

[130] *Id*. at 2844.

[131] *Id*. at 2844-46

[132] *Id*. at 2845 (internal quotations and citations omitted).

[133] *Id*. at 2846-47 (internal quotations and citations omitted).

[134] *Id*. at 2820 (majority opinion) (citing *Buckley v. Valeo*, 424 U.S. 1, 74 (1976); *Citizens United*, 130 S.Ct. 876, 916 (2009)).

[135] *Id*. at 2822-23 (Alito, J., concurring).

[136] *Id.* at 2836-37 (Scalia, J., concurring).

[137] Justice Stevens and Breyer also express doubts about the as applied challenge: "[f]or an as-applied challenge to a law such as the [Public Records Act] to succeed, there would have to be a significant threat of harassment directed at those who sign the petition that cannot be mitigated by law enforcement measures." *Id.* at 2832 (Stevens, J., concurring). The justices "demand strong evidence before concluding that an indirect and speculative chain of events imposes a substantial burden on speech. A statute is not to be upset upon hypothetical and unreal possibilities, if it would be good upon the facts as they are." *Id.* at 2831-32 (internal quotation marks omitted).

[138] Buckley v. Valeo, 424 U.S. at 74.

[139] *See* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 100 (1982) (detailing evidence of FBI surveillance, employer retaliation, threatening phone calls and hate mail, burning of group's literature, and destruction of group's property in affirming as-applied challenge to disclosure law brought by a Socialist political party).

[140] Doe v. Reed, 130 S.Ct. at 2820 ("those resisting disclosure can prevail under the First Amendment if they can show 'a reasonable probability that the compelled disclosure [of personal information] will subject them to threats, harassment, or reprisals from either Government officials or private parties.'"). The Supreme Court similarly stated, discussing Buckly v. Valeo, in Citizens United v. FEC, 130 S. Ct. 876 (2010), that "the Court acknowledged that as-applied challenges would be available if a group could show a reasonable probability that disclosure of its contributors names will subject them to threats, harassment, or reprisals from either Government officials or private parties." *Id.* at 914 (internal quotations omitted).

[141] Buckley v. Valeo, 424 U.S. at 70-71; s*ee also* FEC v. Hall-Tyner Election Campaign Comm., 678 F.2d 416, 420 (2d Cir. 1982) ("There is a paramount public interest in maintaining a vigorous and aggressive political system which includes even participants whose ideologies are abhorrent to that system. This principle repels totalitarianism and the rise of dictators by permitting even those whose views are anathema to ours to partake in the dynamics of an open and vigorous election without fear of reprisal. Acknowledging the importance of fostering the existence of minority political parties, we must also recognize that such groups rarely have a firm financial foundation. If apprehension is bred in the minds of contributors to fringe organizations by fear that their support of an unpopular ideology will be revealed, they may cease to provide financial assistance. The resulting decrease in contributions may threaten the minority party's very existence. Society suffers from such a consequence because the free flow of ideas,

the lifeblood of the body politic, is necessarily reduced. . . . Privacy is an essential element of the right of association and the ability to express dissent effectively. . . . [F]orced revelations would likely lead to vexatious inquiries which consequently could instill in the public an unremitting fear of becoming linked with the unpopular or the unorthodox."(internal quotation marks omitted)).

[142] *See, e.g., Gay Marriage May 24, 2010*, GALLUP, http://www.gallup.com/poll/128297/Gay-Marriage-May-2010.aspx (last visited Dec. 13, 2010).

[143] *See* Doe v. Reed, 130 S.Ct. at 2827 (Sotomayor, J., concurring); *id.* at 2836-37 (Scalia, J., concurring).

[144] *Id.* at 2819 (majority opinion) ("States allowing ballot initiatives have considerable leeway to protect the integrity and reliability of the initiative process, as they have with respect to election processes generally."); *Id.* at 2827 (Sotomayor, J., concurring) ("States enjoy 'considerable leeway' to choose the subject that are eligible for placement on the ballot and to specify the requirements for obtaining ballot access . . . .").

[145] *Id.* at 2834-35 (Scalia, J., concurring).

[146] *Id*. at 2836-37.

[147] *See Id.* at 2827 (Alito, J., concurring) (suggesting that the secretary of state could check for duplicate signatures using a digitized copy of the submitted petitions, as well as, digitally cross check the names and addresses on the petition with those found on the statewide voter registration database); *Id.* at 2840-42 (Thomas, J., concurring) (stating that Washington could easily create a digital database of the submitted petitions where state officials could verify voter registration, check for duplicate names, and even allow individual citizens to determine if their name had been fraudulently placed on a petition).

[148] *See* CAL. ELEC. CODE § 18650 (Deering 2009).

[149] H.B. 2277, 60th Leg., Reg. Sess. (Wash. 2007) ("An act relating to encouraging initiatives and referenda by extending privacy protections to signatories and assuring accurate verification. . . .").

The Ambiguous "*Right To Privacy*": Launching Australia's Privacy Law Into The 21st Century

By Caroline Bush, S. Stuart Clark, and Amanda Graham

LIKE many of its western counterparts, Australia worships at the altar of celebrity. As such, it is not uncommon for the personal misadventures of some of its more famous citizens to feature on the pages and websites of the mass media. While there are many examples of this phenomenon, an incident that the Australian public found particularly engrossing occurred in March 2010 when pictures of Lara Bingle, a minor celebrity who featured in a recent Australian tourism promotion in the United States and former fiancée to an Australian Professional Cricket star, brought Australia's ambiguous lack of a general right to privacy back into sharp focus.

The incident involved photographs taken of Ms. Bingle, without her consent, while she was in the shower. The photographs were published in a popular Australian women's magazine and the fact of their existence featured prominently in the Australian mass media. Ms. Bingle threatened legal action against the photographer and distributor of the photo, a former professional football star for a breach of her privacy.[1] Unfortunately for Ms. Bingle, the current status of privacy laws within Australia is such that her prospects of successfully prosecuting such an action are slight.

The fact is that Australia's privacy laws (and the common law surrounding them) are a work in progress. In particular, Australia's federal privacy legislation is undergoing its most significant reforms since it was introduced in 1988. Notably, amidst a mass of reform proposals being considered is the introduction of a statutory cause of action for serious breach of privacy. In time, there is the prospect that those in situations similar to Ms. Bingle may have redress through a cause of action the existence of which is intended to prevent breaches in the first place and compensate those who suffer if breaches nonetheless occur.

The scale of reform being considered in Australia is considerable. As such, this paper will only outline the reform process over the last several years at a federal level and detail the progress that is presently being made towards the next chapter of privacy law in Australia. The

Caroline Bush is a partner in Clayton Utz's Canberra office. She is a litigator with a particular focus on public law issues including complex regulatory matters, freedom of information and privacy as well as administrative decision-making by Australian Government agencies.

Stuart Clark is a partner with Clayton Utz and an Adjunct Professor at Macquarie Law School in Sydney. He is a litigator with a particular interest in the defence of class actions and complex litigation. He has been a member of the IADC since 1993.

Amanda Graham is an associate with the Clayton Utz public law group in its Canberra office.

current status of the reforms will be considered, including a brief discussion of some key aspects of those reforms, including the introduction of the so called Australian Privacy Principles and the proposed introduction of a cause of action for a serious breach of privacy.

I. Background and context of the Australian privacy environment and reform

At a national level, the legislation regulating privacy is the *Privacy Act* 1988 (Cth) (Privacy Act) and it is its reform that is the focus of this paper. Australia's federal Privacy Act regulates the management of personal information through a series of broadly stated principles set out in the Privacy Act, with a particular focus on the collection, use and disclosure, retention and access to personal information. The Privacy Act applies to the federal government and its associated departments and agencies (through the Information Privacy Principles) and certain private sector organizations (through the National Privacy Principles). As Australia is a federation, privacy law in Australia is also necessarily fragmented between federal, state and territory legislation and indeed other content-related legislation such as the New South Wales *Health Records and Information Privacy Act.*

On 31 January 2006, the Australian Government instructed the Australian Law Reform Commission (ALRC) to conduct a review of Australia's privacy law regime. The ALRC is a federal government agency that is tasked with reviewing Australia's laws with a focus on ensuring greater access to justice by "*making laws and related processes more equitable, modern, fair and efficient.*"[2]

The key focus of the review was to consider "*the extent to which the Privacy Act 1988 and related laws continue to provide an effective framework for the protection of privacy in Australia.*"[3]

In August 2008 the ALRC released its report "*For Your Information: Australian Privacy Law and Practice*" (ALRC Report). The general tenor of the report was that, while the Privacy Act has been effective in the past, there is a need for reform in order to bring it up to date with the information age. The Federal Government delivered a two-stage response to the 295 recommendations in the ALRC Report.

The first stage response was released in October 2009 entitled, "*Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108*" (First Stage Response). It is primarily concerned with replacing the existing Information Privacy Principles and National Privacy Principles contained in the Privacy Act with a single set of uniform Australian Privacy Principles. These will apply to Government agencies and private sector organisations alike. They will become the cornerstone of Australia's privacy protection framework. In June 2010, the Federal Government released the Exposure Draft of the legislation intended to implement this First Stage Response. The Senate Finance and Public Administration Committee is considering the Exposure Draft. It will report in July 2011.

II. Reform - First Stage Response to ALRC

The First Stage Response deals with 197 of the recommendations. These were largely accepted by the Government. A key theme is the recognition of the need to balance, on the one hand, the protection of personal information in an appropriate manner given the evolving information age, with, on the other hand, the need to ensure that government and business efficiency is not overly restricted.

The Companion Guide to the Exposure Draft for the First Stage Response (Companion Guide), states that "*Australians deserve a modern privacy law, which provides robust protections about the collection and use of our personal informati*on" and that the purpose of the reform is "*revitalising the law for the 21st Century.*"[4] As such, it is clear that the reform is particularly seeking to address certain deficiencies in the current privacy law regime which do not adequately deal with privacy issues that arise in the information age.

A. The Australian Privacy Principles

That said, the Exposure Draft only deals with implementing the Australian Privacy Principles, recommended by the ALRC. However, this is only one of four key aspects that are to be introduced as part of the first stage of the reform. With this in mind, it may be some time before Australia's privacy laws are appropriately brought into the 21st century.

The Australian Privacy Principles outlined in the Exposure Draft are intended to replace the existing Information Privacy Principles, which apply exclusively to government agencies and departments and the National Privacy Principles which apply exclusively to selected private sector organisations. The Australian Privacy Principles will create a uniform set of principles that will apply equally to the public and private sector when dealing with personal information.

The acceptance of the ALRC recommendations for the adoption of uniform principles is an affirmation by government that an overly prescriptive approach to privacy regulation is not appropriate. Rather, a principles-based approach is more likely to evolve to meet the privacy challenges that will continue to arise with the information age as technology changes. A principles based approach acknowledges that high level guidelines and generally stated principles provide protection to personal information while providing agencies and organisations with the ability to tailor personal information handling practices to their individual needs and technology practices.

In particular, it is intended that the privacy principles should continue to be technology neutral.[5] That is they should not be directed at any specific technology but rather should state principles of general application. The principles should be sufficiently flexible to ensure that personal information stored in all mediums, including those not yet anticipated, will be protected and that the principles need to remain current in the context of an ever evolving technological environment.

The Australian Privacy Principles are structured to address each stage of the information-handling process. They address openness (relating to general privacy policies and practice), anonymity and pseudonymity, collection, dealing with unsolicited information, notification, use and disclosure, direct marketing, cross-border disclosure, dealings with government-related identifiers, data quality, data security and access to and correction of personal information. Set out below is a summary of the effect of the proposed Australian Privacy Principles.

1. Openness

An Openness Principle will require agencies and organizations to set out a clearly expressed privacy policy that details how that entity collects, holds, uses and discloses personal information (i.e. how it handles personal information at all stages of the information cycle).

In addition to improving transparency of the management of personal information, this is designed to ensure that organizations are aware of their privacy obligations and are integrating ways to conform to these obligations from the point of designing and developing the information systems that collect and manage the personal information.

The Openness Principle also has an inward-looking focus. The Principle will require agencies and organizations to take reasonable steps to develop and implement internal policies and practices that enable and promote compliance with the Australian Privacy Principles. This includes activities such as the training of staff about privacy practices and the establishment of procedures to receive and respond to privacy complaints and enquiries.

2. Anonymity and Pseudonymity

This principle will require agencies and organizations to give individuals the option to interact anonymously or pseudonymously, where it is lawful and practicable in the circumstances. A similar obligation currently exists in National Privacy Principle 8. This new Principle will extend that obligation to government agencies.

The Privacy Commissioner will be given the function of developing and publishing guidance the operation of this Principle, especially regarding when it is "*lawful and practicable*" to allow information to be given anonymously or pseudonymously. This is vital, given that anonymous or pseudonymous interactions will likely not be practicable for the delivery of government services, benefits and entitlements as well as in investigative contexts.

3. Collection

A broadly framed Collection Principle will ensure that: "*entities must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities (the functions test).*"[6]

The Government has argued that this will assist in ensuring that the individual is aware that their personal information is being collected and that the information is

as accurate, complete and up-to-date as possible.

There are public interest exceptions to this general Collection Principle, which allow for the collection of personal information in circumstances which involve assisting: in times of emergency; in carrying out war or peacekeeping operations; in the location of missing persons and collection for diplomatic or consular processes.

The Exposure Draft has also proposes a principle that deals with the receipt of unsolicited personal information and the collection of sensitive information. Where an agency or organization receives unsolicited personal information, it must either (if lawful or reasonable to do so):

- destroy the information as soon as practicable; or
- alternatively comply with the Australian Privacy Principles that apply to the information in question as if the agency had taken active steps to collect that information.

The Government will encourage the development and publication of guidance by the Privacy Commissioner as to:

- when it is, and is not, reasonable and practicable to obtain personal information from another source; and
- the meaning of "*unsolicited personal information*".

4. Notification

The Notification Principle will require an agency or organization, at the time of collecting personal information, to take reasonable steps to notify or otherwise ensure that the individual, the subject of the personal information, is aware of numerous issues. In particular, the notification will include details of the facts and circumstances of collection (if the individual is not aware that personal information was collected), the purpose of collection, rights of access to and correction of the information, third parties to which similar information is usually disclosed, and relevant privacy complaint handling mechanisms. Agencies and organizations should also take steps to notify individuals, if their personal information is reasonably likely to be transferred overseas.

5. Use and Disclosure

The Use and Disclosure Principle will regulate the use and disclosure of personal information. This principle will generally provide that the personal information must not be used for a purpose, other than the purpose that it was collected for, unless the individual has consented to its use for another purpose.

There are however some public interest exceptions that will apply to this principle, notably including circumstances where an agency reasonably believes that certain use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public.

6. Direct Marketing

The Government has agreed with the ALRC's recommendation that the Australian Privacy Principles should also regulate "*direct marketing*" in a discrete, stand-alone Privacy Principle (separate from the Use and Disclosure Principle, under which it is currently regulated in the National Privacy Principle). The key to the principle is that a person's consent is required in various circumstances and that people must have choices to opt out.

Different rules will apply to direct marketing practices depending upon whether the information proposed to be used for direct marketing purposes is sensitive information (for example, information about a person's race or political opinions or sexual preference), in which case you need consent and depending upon whether the information was collected by the entity that is actually using it for direct marketing purposes, or by another entity.

This principle also requires that when using direct marketing, individuals must be given a means by which they can request not to receive direct marketing communications.

7. Access and Correction

In its First Stage Response, the Government indicated that there would be an Access and Correction Principle that contains an enforceable right to access and correct an individual's personal information that is held by an agency or organization. In the subsequent Exposure Draft, the proposed Access and Correction Principle was broken into two independent principles, one in relation to *access* and the other in relation to *correction*.

The Companion Guide suggests that the purpose of the proposed Access Principle is "*to ensure that individuals have access to personal information that entities hold about them and can correct the information where it is inaccurate, irrelevant, out-of-date or incomplete*".[7] The principles also provide some limitations on an individual's general right of access to their personal information. The degree and scope of these limitations will depend on whether the information is held by an agency or organization. An individual will be entitled to access personal information held by an agency, except to the extent that the agency is required or authorized to refuse to provide access under a federal law (for example, where the FOI Act provides that a particular document is exempted from disclosure). An organization will be obliged to provide access to personal information except to the extent one of the public interest factors identified in subsection (3) of the proposed principle applies.

Similarly, the proposed Correction Principle creates an obligation for entities to take reasonable steps to "*correct personal information if it is inaccurate, out-of-date, incomplete or irrelevant*".[8] This Principle will also impose an obligation on the entity to notify certain other entities to which the information has been disclosed, of the relevant changes (providing the individual has requested that this notification occur).

There is significant overlap between the *Freedom of Information Act 1982* (FOI Act) and the Privacy Act with respect to accessing and correcting of

personal information held by agencies. The Government proposes that the Access and Correction Principle (now two separate principles) will be the primary means of access to, and correction of, an individual's own personal information. The focus of the FOI Act is thus intended to be on access to documents other than an individual's own personal information. However, many of the FOI Act's rights to access and correct personal information will be retained, given that most documents containing personal information will also contain personal information of third parties and non-personal information.

8. Identifiers

While noting the potentially intrusive capacity of government related identifiers, the Government clearly feels that those identifiers serve as effective tools for identifying and linking personal information and have sought to strike a balance between these competing imperatives. The core purpose of the principle Identifiers Principle is essentially to ensure that government related or issued identifiers do not become "*de facto national identity numbers*"[9].

The principle will seek to restrict organisations (as distinct from government agencies) from using government related identification numbers as their own identifier of an individual. The kinds of identifiers that are affected are, for example, numbers such as a driver's licence number or a Medicare number.[10] The principle is also intended to prohibit the use of government related identifiers for the purposes of data-matching of information that is held by other organisations.

This principle will not however restrict an organisation's use of government related identifiers for the purposes of verifying the identity of an individual. The Companion Guide provides an example of an appropriate use of identifiers by organisations and states that: "*the principle is not intended to prevent a courier service from checking a person's driver's licence to ensure that a parcel is being delivered to the correct recipient.*"[11]

9. Data Quality

A Data Quality Principle will oblige agencies and organizations to take reasonable steps to ensure that personal information they collect, use and/or disclose is accurate, complete, up-to-date and relevant, in light of the purposes of collection, use or disclosure.

The steps that must be taken are "*reasonable steps.*" This indicates that a proportional approach will be taken to compliance with the principle, having regard to the actual purpose of collecting, using or disclosing the information.

10. Data Security

A Data Security Principle will oblige agencies and organizations to protect the personal information that they hold from misuse, loss and unauthorized access, modification or disclosure. In particular, the principle will require the taking of reasonable steps to destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed and

retention is not required or authorized by law. The Government sees this as an effective way to reduce the risk that personal information will be mishandled.

11. Cross Border Data Flow

Finally, the Australian Privacy Principles will include a Cross-border Data Flow Principle designed to bolster the protection offered to personal information that is disclosed to a recipient outside Australia. As stated in the Companion Guide, the principle is intended to ensure that: *"… the obligations to protect personal information set out in the Australian Privacy Principles cannot be avoided by disclosing personal information to a recipient outside Australia."*[12]

The principle provides that before disclosing personal information to a person who is not in Australia, unless a relevant exemption applies, the entity must take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach the Australian Privacy Principles in relation to the information. While it is not stated in the principle itself, it is thought that the relevant steps in most cases are likely to comprise contractual obligations to comply with the Australian Privacy Principles.

The principle will provide that an agency or organisation that discloses personal information to a recipient outside Australia will also be accountable for that information unless an exemption applies. A notable exemption contained in the principle applies if an overseas recipient of the relevant personal information is subject to a law or binding scheme in their own jurisdiction which is substantially similar to the Australian scheme in terms of its protection of personal information.

If an exemption applies, the recipient will essentially become responsible for the personal information. However, if the Australian agency or organization remains accountable, any act by the recipient that would be an interference of privacy if committed in Australia is taken to have been an act of the Australian agency or organization.

B. What else will happen in the First Stage?

The other anticipated reforms that will be addressed as part of the First Stage Response include reforms for enhancing protection for credit reporting and health information and clarifying the Privacy Commissioner's powers and functions. From 1 November 2010, the role of the Privacy Commission has come under the umbrella of the newly created Office of the Australian Information Commissioner (which is also responsible for Australia's FOI laws). The Government has indicated that the First Stage Response will be introduced in parts and we can anticipate Exposure Drafts of legislation dealing with these topics once the form of the uniform privacy principles are finalised.

III. Reform - Second Stage Response to ALRC

It is anticipated that the Government will issue the Second Stage Response after the First Stage Response has been fully implemented (which as noted above

will, of itself, involve considerable legislative reform).

The Second Stage Response is likely to focus on the remaining 98 recommendations in the ALRC Report, and it is largely accepted that these recommendations are the more controversial issues that were raised in the ALRC Report. These issues include:

- proposals to clarify or remove certain exemptions from the Privacy Act;
- introducing a statutory cause of action for serious invasion of privacy;
- serious data breach notifications;
- privacy and decision making issues for children and authorised representatives;
- handling of personal information under the *Telecommunications Act* 1997; and
- national harmonisation of privacy laws (partially considered in stage one).

The Government has not yet made it clear the degree to which the Government is likely to accept or reject the relevant recommendations within the ALRC Report.

The First Stage Response could be described as largely uncontroversial. Of the 40 submissions made in relation to the Exposure Draft there appears, on the whole, to be a good deal of support for the proposed amendments with many submission proposals relating to terminology and clarification, rather than substantive policy changes. It is anticipated that the Second Stage Response will attract significantly more debate.

IV. Watch this space - an action for breach of privacy?

As already observed, Australia does not have a right to privacy that is readily enforceable and compensable in Australian courts.[13] The issue of whether there is a general or common law "*right to privacy*" has been considered by a number of Australian courts, which have, in effect, determined that, at this point in the evolution of the common law, there is no general right to privacy under Australian law. Notwithstanding this, Australian courts have been inclined, in a handful of cases, to allow, what is in effect a claim for damages caused by what may be described as a breach of privacy.[14]

To remedy what it regarded as a lack of a clear common law cause of action enforceable in the courts, the ALRC recommended the introduction of a cause of action for a breach of privacy. The recommendation provides that, in order to establish the cause of action, a claimant must show:[15] "*(i) there is a reasonable expectation of privacy; and (ii) the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.*"

The recommendation also provides that, when determining whether the cause of action can be established, the relevant court must consider "*whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression).*"[16]

Other characteristics of the recommendation include that the cause of action would only be able to be brought by natural persons, it would be actionable without proof of damage, and would be restricted to intentional or reckless acts on the part of the respondent. The recommendation also suggests that the appropriate remedies should include damages, account of profits, injunctions and correction orders.

There are two key areas of debate that are likely to arise in the context of the possible introduction of a cause of action for a breach of privacy. The first is whether the creation of a cause of action for breach of privacy, is appropriate in light of concerns that the action may have implications for freedom of expression (journalists have naturally spoken out against the need for such a cause of action and indicated what they see as the risks of impeding their freedom to publish particularly with respect to "public" figures). The second will revolve around the form that any cause of action should take and the extent to which the public interest will feature.

Interestingly, the New South Wales Law Reform Commission has also recently considered the introduction of a cause of action for a breach of privacy in the context of the New South Wales Privacy Act.[17] The New South Wales proposal is much broader[18] omitting the "*highly offensive*" requirement from the necessary elements, and limiting the public interest defence such that it would only require that regard be had to the relevant public interest (as distinct from the requirement intended to be included in the cause of action recommended by the ALRC which would require that the "*claimant's privacy outweighs other matters of public interest*").

The debate over the introduction of a cause of action for breach of privacy has only just begun in Australia and it is not known how the current administration will react. Of course, even if the cause of action is enacted, Australian judges will be required to rule on the statutory criteria set out in the legislation. Their perceptions of the need to balance freedom of expression (which is only partially enshrined in Australia in an implied constitutional right of freedom of political communication) and the need for privacy will be important in the evolution and effectiveness of any cause of action. Critically however, the mere existence of the cause of action may give individuals and organisations some pause for thought before embarking upon some of the more gratuitous invasions of privacy. Indeed it is this very fact that has journalists and commentators concerned.

V. Conclusion

Australia is in the midst of launching its most significant reforms to the national privacy regime since the introduction of the Privacy Act in 1988. It is clear from the Exposure Draft that it is the Government's intention to develop a regime which allows Australia to appropriately deal with the multiplicity of privacy issues that arise in the age of information in a fashion which is intended to be technology neutral. However, given that the current Exposure Draft deals with only a fraction of the least controversial recommendations made within the ALRC Report, and it is unlikely that these proposals will receive

legislative implementation until the end of 2011, it is clear that dragging Australia's privacy law into the 21st century will be a time consuming and possibly difficult process.

[1] Gordon Farrer, *Bingle photo privacy poser*, THE AGE (Melbourne), 3 March 2010, http://www.theage.com.au/victoria/bingle-photo-privacy-poser-20100302-pgfo.html.
[2] *About the ALRC*, Australian Law Reform Commission <http://www.alrc.gov.au/> at 14 December 2010.
[3] *See* 'Terms of Reference', AUSTRALIAN LAW REFORM COMMISSION, *For Your Information: Australian Privacy Law And Practice*, Report 108 (2008) (ALRC Report).
[4] 'Companion Guide: Australian Privacy Principles', Australian Government, June 2010, pages 2-3.
[5] See Recommendation 18-1 of the ALRC Report, page 34 and the First Stage Response page 6.
[6] See the Companion Guide, page 10.
[7] See the Companion Guide, page 14.
[8] See the Companion Guide, page 14.
[9] See the Companion Guide, page 13.
[10] Medicare is Australia's universal healthcare system.
[11] See the Companion Guide, page 14.
[12] See the Companion Guide, page 12.
[13] Albeit that there is a mechanism in the Privacy Act whereby a person can make a complaint to the Australian Privacy Commissioner (who is not a judicial officer) about an interference with privacy (commonly comprising a breach of a relevant privacy principle) and the Commissioner can make a determination in relation to the complaint (which can be enforced if the respondent to the complaint does not comply with the determination).
[14] *See in particular* Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd. (2001) 208 CLR 199; Doe v. ABC and Ors [2007] VCC 281; *and* Giller v. Procopets [2008] VSCA 236.
[15] AUSTRALIAN LAW REFORM COMMISSION REPORT 108 - *For your Information*, 11 August 2008, Recommendation 74-2, p. 2584.
[16] AUSTRALIAN LAW REFORM COMMISSION REPORT 108 - *For your Information*, 11 August 2008, Recommendation 74-2, p. 2584.
[17] New South Wales being the largest state of the Australian federation.
[18] NEW SOUTH WALES LAW REFORM COMMISSION, Report 120 - Invasion of Privacy, April 2009.

Voyeurism in the Computer Age: A School District's Experience

By Basil A. DiSipio, John J. Bateman and Lorraine B. McGlynn

A NEW JERSEY college student leapt to his death from the George Washington Bridge after learning that his roommate had streamed live video to the internet of his sexual encounter with another student. The footage was allegedly broadcast from a webcam secretly activated in the students' shared dormitory room. The roommate and another student have been charged with invasion of privacy and have reportedly withdrawn from school. The case has attracted international attention, prompting anew concerns about how best to deal with the effects of carelessly used technology. But what if the school was the accused? That question was raised in *Robbins v. Lower Merion School District,*[1] and *Hasan v. Lower Merion School District,*[2] a pair of highly publicized civil lawsuits filed early last year in a federal court in Pennsylvania. The actions forced Lower Merion School District to defend itself against claims of cyberspying. It is a cautionary tale in which the student became the teacher, of lessons learned about privacy and property rights and the unforeseen consequences of new technologies on both. The school district might argue that the now resolved litigation is proof that the road to hell is paved with good intentions. The students, that cyber-bullying exists at the institutional level. The reality is both may be correct.

According to court documents, Lower Merion School District, located in an an affluent Philadelphia suburb, had issued to every one of its more than 2000 high school students an Apple MacBook laptop equipped with an integrated webcam. LANrev computer management software installed on the laptops enabled them to communicate with the Lower Merion server when connected to the internet. The LANrev software included "TheftTrack," a feature that could be remotely activated. Capable of locating the Internet Protocol address for the laptop's internet connection and of simultaneously photographing both whatever appeared in front of the webcam and on the computer screen, a "screenshot," TheftTrack could be set to record the images at timed intervals. Its purpose was to assist in the recovery of lost or stolen laptops. Lower Merion did not inform its students or their families that the laptops had this functionality. So neither student nor family would ever be aware that the TheftTrack feature had been activated.

Student Blake Robbins alleged that in the fall of 2009, a Lower Merion assistant principal accused him of improper behavior while at home, confronting him with an image of himself obtained from his laptop's webcam. It was then that he and his parents first learned that Robbins' computer was equipped with TheftTrack and of the

Basil DiSipio is managing shareholder and John Bateman and Lorraine McGlynn are shareholders of Lavin, O'Neil, Ricci, Cedrone & DiSipio. Mr. DiSipio and Mr. Bateman are IADC members.

school district's covert webcam monitoring. Several months later, Robbins and his parents filed a class action complaint on behalf of themselves and other Lower Merion families alleging that the school district had secretly equipped school-issued laptops with webcams and tracking devices to spy on district students in their homes. Asserted were causes of action for violation of the Electronic Communications Privacy Act, the Computer Fraud Abuse Act, the Stored Communications Act, 42 U.S.C. §1983, the Pennsylvania Wiretapping and Electronic Surveillance Act, in addition to constitutional and common law claims for invasion of privacy. Two days after the Robbins complaint was filed, the school district discontinued the use of TheftTrack.

On the day after that, the Robbins family moved for a temporary restraining order prohibiting the school district from remotely activating the webcams, contacting members of the putative class, taking possession or altering the student-issued laptops, and destroying evidence. The American Civil Liberties Union quickly joined the fracas, seeking permission to file an amicus brief in support of the issuance of a TRO. A decision on the TRO was averted by the entry of an order stipulated by the parties prohibiting the remote activation of the cameras, the destruction of evidence, and communication by the school district with Lower Merion students with respect to the lawsuit's allegations.

The school district acknowledged installation of the anti-theft software on the computers, but denied that it was used in conjunction with the webcam to conduct illegitimate surveillance of students or to collect images for illicit purposes. Forensic computer experts hired by both sides descended on the school district to sift through evidence in its electronic files. With each passing day, the recriminations mounted. The FBI and U.S. Attorney's Office, acting in conjunction with local and county officials, launched a federal investigation. The U.S. Department of Justice issued a statement that "[t]he issues raised by these allegations are wide-ranging and involve the meeting of the new world of cyberspace with that of physical space. Our focus will be on whether anyone committed any crimes." Amidst the turmoil, two groups of intervenors, backed by a substantial percentage of district parents, sought to join in the Robbins action requesting the prohibition of any further activation of the webcams and proscribing the dissemination of images already collected. Some parents also requested an order banning press interviews near the school or students' homes to quell the media frenzy that surrounded the litigation.

The facts were soon revealed.[3] The software had been activated on more than 175 occasions by one or both of two district information services employees. The employees had permission to trigger the feature but no distinct guidelines for its use. The report from the school district's internal investigation noted that "[t]he informal procedures that [the employees] used varied over time and were not followed consistently." Report at 2. At least 58,000 images of district students had been captured by webcams, including hundreds of Blake Robbins. One in which Robbins is pictured sleeping was released to the media. It

was also discovered that there were instances in which the software was not deactivated for extended periods of time, even after a laptop thought missing was located. Jalil Hasan[4] claimed to be one of the students affected by the district's failure to turn the webcam off, filing his own suit asserting the same causes of action as Robbins.

While Lower Merion was busy dealing with the maelstrom created by the exposure of its clandestine activities, another entity weighed in. Its insurer, denying coverage for conduct it characterized as "a non-consensual, surreptitious, remote visual voyeurism inside the claimant's own home," filed its own action seeking a declaration that it owed Lower Merion neither a defense nor indemnity.[5] It claimed that its coverage was for claims of personal injury, not invasion of privacy. As a result, the taxpayers of Lower Merion were facing a double threat, to their privacy and their pocketbooks.

The school district was contrite. It admitted and apologized for the mistakes made, including the failure of its administration to fully appreciate the privacy concerns implicated by tracking students using webcam capabilities. It pledged full disclosure of its past and future technological actions with respect to the laptops and set to work drafting policies and procedures. The Court ordered that parents and students whose images had been collected be notified and given an opportunity to view the images. It also directed the school district to pay interim fees and costs to counsel for Robbins and Hasan of about a quarter of a million dollars. At that point, the school district's own defense was reportedly hovering around the million dollar mark.

Ultimately, the school district was cleared of criminal wrongdoing. The U.S. Attorney's Office announced that it had "not found evidence that would establish beyond a reasonable doubt that anyone involved had criminal intent." The school district's insurer also reversed its initial decision denying coverage for the civil litigation, agreeing to shoulder $1.2 million of the fees and costs associated with the litigation. Eight months after they were commenced the cases settled for $610,000; $175,000 to Robbins, $10,000 to Hasan and $425,000 to their attorney. The Court permanently enjoined Lower Merion from: remotely activating webcams on school-issued computers; purchasing software, hardware or any other technology that allowed for the remote activation of webcams on student laptops or the remote monitoring or recording of audio or video from student laptops; capturing screenshots; accessing or reviewing any student-created files contained on student laptops, including emails, photographs, instant messaging records, internet usage logs and web browsing histories, except as explicitly allowed by the district's newly adopted policies or by parental consent; and viewing, disseminating or permitting access to images already gathered. The order did not ban the use of global positioning systems or other anti-theft tracked technology outright, but mandated conspicuous, written disclosure of its functionality and usage and student and parental consent.

With its new-found appreciation of the paradoxical virtues of transparency and privacy, the written measures

implemented by Lower Merion are odes to both.[6] In addition to requirements mandating disclosure and consent for the use of any tracking technology and a proscription against using webcams for that purpose, the regulations forbid remote access to student laptops except to resolve technical problems or when a laptop is reported missing or stolen by written report filed with the district. If permission for remote access is given, a record of the time, date and duration of the access will be generated. As for personal files saved to a student's computer, district personnel may access them only with express, written consent or after the laptop is permanently returned, at the end of the year or otherwise, after the opportunity for removal of student files is given. An important caveat is that if a "reasonable suspicion" exists that a student has violated the law, district rules, or policies, the laptop can be confiscated, but not remotely accessed, and the files may be reviewed by district personnel. Student data stored on the district's network, however, is fair game. "Students have no expectation of privacy in any material or information stored on, created on, accessed through or transmitted through [the school district network]."[7]

Other policies ratified by Lower Merion as a result of the imbroglio address the chain of school district authority for dealing with laptop issues.[8] They mandate technology training for administrators, teachers, computer support personnel and anyone else involved with the laptops. Their implementation speaks to the charge that ignorance of the capabilities of technology and its uses are culpable, even in the absence of illicit intent. They also address the danger of supervisory personnel abdicating responsibility for computer-related issues and reposing the administration of information services in the hands of technicians who are unaware of the ramifications of their actions, or worse yet, intent on spying.

There was no shortage of hyperbole during the pendency of the litigation. The plaintiffs labeled TheftTrack "peeping tom technology." Commentators lambasted Lower Merion for spying on children and suggested that child pornography charges be considered. Others blamed school district hubris, castigating Lower Merion as an authoritative bully with little regard for the privacy of its students or the law. With the benefit of hindsight, rogue seems a harsh adjective for Lower Merion's activities, though surreptitious they undeniably were. Perhaps better explained as a case of bad judgment, poor training, or both, the school district's experience teaches that covert activities, no matter how well-intended, can have far-reaching implications. Complacency in technological affairs is simply not an option.

In our brave new world, the right to privacy is often juxtaposed against increasingly more invasive technologies which serve as effective weapons in law enforcement. From global positioning systems in cars, cell phones, and computers to airport scanners, innovation often comes at the price of anonymity. While presumptive confidentiality may be a thing of the past, the expectation of privacy cannot be ignored. The Lower Merion melee sparked interest from legislators, like then Pennsylvania

Senator Arlen Spector, who suggested that any gap in wiretap laws be closed to address privacy concerns wrought by technological advances. The law may eventually catch up with present day capabilities, but, as Lower Merion discovered, existing common law principles and legislative enactments are of limited utility as guideposts for the use of technology. The boundaries of the right to privacy are elusive and as the technology continuum advances emerging applications may outgrow the legal paradigm adopted. The risk is great that any individual, institution, business, employer, and organization engaged in computer-based covert surveillance may be accused of cyberbullying, civil rights violations, criminal conduct and more. Disclosure is therefore the watchword for the future. It is a lesson Lower Merion paid dearly to learn.

---

[1] No. 10-0665 (E.D. Pa. 2010).
[2] No. 10-3663 (E.D. Pa. 2010).
[3] The report of the school district's internal investigation conducted by the law firm of Ballard Spahr in association with computer forensic consultant L3 Services, Inc. is available at the district's website at http://www.lmsd.org/sections/laptops/default.php?&id=1258.
[4] *Id.*
[5] Graphic Arts Mutual Insurance Co. v. Lower Merion School District, No. 10-1707 (E.D. Pa. 2010).
[6] No. 10-1707 (E.D. Pa. 2010).
[7] The newly adopted policies are available at the school district's website at http://www.lmsd.org/sections/laptops/default.php?t=pages&p=laptops_docs.
[8] *Id.*

The Privacy Implications and Legal Footing of Arizona's Immigration Law: S.B. 1070

By Steven J. Strawbridge and Bryan S. Strawbridge

. . . It hit at the clever homeless portion of the population which wasn't tied down to anything. In the early stages, people made many mistakes with those passports—and those not registered at their places of residence, and those not registered as having left their former places or residence, were raked into the Archipelago, if only for a single year.

And so the waves foamed and rolled.[1]

I. Introduction and Overview of S.B. 1070

ON APRIL 23, 2010, Arizona Governor Jan Brewer signed into law state Senate Bill 1070 ("S.B. 1070").[2] Although the statute's numeric designation may not be a household name, few are unaware of Arizona's controversial new immigration law, which mandates that all law enforcement officials shall take steps to verify the immigration status of any individual with whom they come in contact if there exists reason to suspect that the individual is in violation of federal immigration laws.[3] With little time and great fanfare, S.B. 1070 was propelled by the media to the forefront of national attention, spurring punditry and protest. It became immediately and undeniably clear that the public had varied opinions as to the efficacy, legality, and scope of the legislation. Many proclaimed the law as being a necessary step to stem the tide of illegal immigration, especially in an economy with near double digit unemployment rates. However, others demonized the legislation as a discriminatory, isolationistic, and flat out un-American attempt to rectify a serious and growing concern, while reminding others of 1930s era fascism. While S.B. 1070 is, of course, limited to the state of Arizona, at least two dozen other states are considering similar enactments.[4]

Steven J. Strawbridge is a Member of Frost, Brown Todd, LLC, in Indianapolis, Indiana, and is the Chair of the Fidelity and Surety Committee of the IADC.

Bryan S. Strawbridge is an Associate with Krieg DeVault, LLP, in Indianapolis, Indiana. All comments and opinions expressed herein are the authors' own.

In the markets of human and drug smuggling, Arizona is the United States' leading brokerage house.[5] With approximately 460,000 illegal immigrants currently residing in Arizona, the impact of S.B. 1070 is by no means insignificant.[6] The existence of these realities has not gone unnoticed by the Arizona electorate. Polls taken on immigration issues in the state routinely show that the majority of residents favor the law as well as an increase in enforcement.[7] As noted by Miriam Jordan in a recent *Wall Street Journal* article:

> Frustration over illegal immigration has been mounting in the state in recent years amid reports of kidnappings and gun battles on the

> state's highways and in the heart of Phoenix. Concerns about the poor economy and unemployment in the state also have contributed to dissatisfaction with illegal immigration.[8]

Awash with aggravation over growing violence and rampant drug trafficking coinciding with the tempest of the national economic catastrophe, Arizona's legislature turned to the comfort of an immigration bill which, according to its supporters, would quell these concerns. According to its detractors, the bill is a knee jerk reaction to a complex problem that cannot be so simply remedied.

This Note will parse the language of the statute, analyze its legality, and provide an overview of the judicial review that has been conducted to date. Finally, this Note advocates for the removal of the legislation from the Arizona code as being an undue burden on civil freedoms and an unconstitutional state attempt to usurp the exclusive federal authority to manage and supervise immigration law enforcement.

II. Provisions of S.B. 1070

Coined the "Support Our Law Enforcement and Safe Neighborhoods Act", S.B. 1070 has shifted immigration laws, which have traditionally been codified as civil statutes, into the realm of criminality.[9] S.B. 1070 has classified mere unlawful presence in the state as a criminal offense, to-wit, criminal trespass.[10] Accordingly, pursuant to S.B. 1070, illegal immigration is a more enforceable and punishable act.[11] The enumerated legislative intent of S.B. 1070 provides:

> The legislature finds that there is a compelling interest in the cooperative enforcement of federal immigration laws throughout all of Arizona. The legislature declares that the intent of this act is to make attrition through enforcement the public policy of all state and local government agencies in Arizona. The provisions of this act are intended to work together to discourage and deter the unlawful entry and presence of aliens and economic activity by persons unlawfully present in the United States.[12]

Although the stated intent of S.B. 1070 appears relatively benign and straight forward on its face, the substantive provisions contained in the legislation have produced significant vitriol.

The Obama Administration's response to the enactment of S.B. 1070 into law was immediate and forceful. President Obama affirmed his displeasure with S.B. 1070 stating that "[t]he Arizona law [threatens] to undermine basic notions of fairness that we cherish as Americans, as well as the trust between police and our communities that is so crucial to keeping us safe."[13] Unsurprisingly, the Mexican Foreign Ministry concurred with President Obama's assessment.[14] However, the sharpest critique of the legislation came from the Catholic Church.[15] Cardinal Roger M. Mahony of Los Angeles said that governmental authorities' ability to demand documents on demand harkened

back to Nazism.[16] "While police demands of documents are common on subways, highways, and in public places in some countries, including France, Arizona is the first state to demand that immigrants meet federal requirements to carry identity documents legitimizing their presence on American soil."[17]

Looking to the specific provisions of S.B. 1070, the act provides the following:

(a) Directs law enforcement to determine the immigration status of ***all*** persons who are arrested as well as those individuals that they reasonably suspect to be illegal aliens during a lawful stop;
(b) Proclaims attrition by enforcement to be Arizona policy;
(c) Permits law enforcement to transfer illegal aliens into federal custody;

- Precludes law enforcement from implementing policies that limit or prohibit enforcement of federal immigration laws; Provides that individuals who provide any federal, state or local identification, which requires verification of lawful status when issued, are presumed to be lawfully present in the United States; Precludes state officials or agencies from implementing constraints on transferring or storing information regarding individuals' immigration statuses, or sharing such information with other federal, state, or local governmental entity for the following purposes:
  - To ascertain eligibility for any public benefit, service, or license provided by the state;
  - To verify a claim of residence if such determination is required by statute or judicial decree; To validate the identity of any detained person; and
  - To establish whether an individual has abided with federal registration laws under the Immigration Nationality Act;[18]

(d) Grants legal residents of Arizona the civil remedy to bring action if they believe a government agency or its policies are in discord with federal immigration laws;
(e) S.B. 1070 is in accord with federal alien registration laws by requiring illegal aliens that violate federal alien registration laws (8 U.S.C. §§ 1304(e), 1306(a)), which require aliens to register and bear their immigration documents at all times) are now subject to arrest and sanction under Arizona criminal laws;
(f) Proscribes citizens from hiring and/or picking up day laborers while impeding traffic;
(g) Prohibits day laborers from soliciting work;
(h) Bans illegal aliens without work authorization from applying for

work, soliciting work in a public place, or working in Arizona;

(i) Illegalizes the transport, harbor, or encouragement of illegal aliens to remain in the United States if the individual knows or recklessly disregards that persons are illegal.

(j) Endorses law enforcement to make warrantless arrests if there exists probable cause to believe the individual has committed any offense which subjects the individual to removal from the country;

(k) Mandates that employers must keep a record of all employees' E-Verify verification for either (a) the employment term or (b) at least three years;

(l) Prescribes impoundment or forfeiture of cars driven by illegal aliens as well as vehicles used to unlawfully transport illegal persons; and

(m) Creates the Gang and Immigration Intelligence Team Enforcement Mission Fund to provide funds to combat gangs and assist in immigration enforcement as well as for reimbursing county jails for costs associated with illegal immigration.[19]

As is readily apparent from the above noted provisions, the scope of reforms contained in S.B. 1070 are expansive. The litigation that resulted challenging the act was expected and immediate.

III. Procedural Background

On July 28, 2010, District Judge Susan R. Bolton of the United States District Court for the District of Arizona significantly weakened the scope and effect of S.B. 1070.[20] Judge Bolton issued a preliminary injunction that precluded the most controversial aspects of the law from taking effect, which was to occur the following day, July 29, 2010.[21] The specific sections, which had been forcefully belied by the act's oppositions, that were enjoined by the injunction, included:

(a) The section which mandated a state officer to make a reasonable attempt at determining the immigration status of an individual stopped, detained, or arrested if the officer has reasonable suspicion that the individual was in the country illegally;

(b) The section which created the crime of soliciting, applying, or performing work as an illegal immigrant;

(c) The section which made it a crime for an individual to fail to apply for or carry "alien registration papers" as required by federal law; and

(d) The section which permitted the warrantless arrest of a person upon the finding of probable cause that the individual has committed an offense punishable by removal from the United States.[22]

However, the injunction does not obviate Arizona public safety officers' discretion that existed prior to S.B. 1070, which they enjoy in choosing whether to assist in the enforcement of federal

immigration laws.[23] Instead, the injunction vitiates the requirement contained in S.B. 1070 that officers are mandated to enforce federal immigration law or face private civil actions.[24]

The actions which led to injunction in the district court were filed by a myriad of individuals, government bodies, and special interest groups, including both public and private actors.[25] Specifically, these plaintiffs included the United States Department of Justice, the American Civil Liberties Union, Phoenix and Tucson law enforcement officials, various municipalities, illegal immigrants individually, and non-profit organizations.[26]

As publicly expressed by Gov. Brewer, the procedural ladder is just beginning.[27] Governor Brewer has proclaimed that "[t]his fight is far from over. In fact, it is just the beginning. . . ."[28] She noted that Arizona intends to "battle all the way to the Supreme Court, if necessary, for the right to protect the citizens of Arizona."[29] However, the official reaction from the Department of Homeland Security ("DHS"),[30] which oversees federal immigration, could not have been more supportive of the court's injunction.[31] The spokesman for DHS stated that the court's decision "correctly affirms the federal government's responsibilities in enforcing our nation's immigration laws."[32] Despite the wholly divergent viewpoints, one consensus can be garnered; both sides concur that legal resolution will not be attained until the Supreme Court issues a dispositive ruling on the issue or a petition for writ of *certiorari* is denied. Either way, conclusion is not likely in the near term. In the interim, analyzing the legal footing of S.B. 1070 is appropriate.

IV. Legal and Policy Critique of S.B. 1070

As a general proposition, the various plaintiffs in the actions challenging the legality of S.B. 1070 have made similar assertions. This Note will focus on three overarching legal arguments made in opposition to the legislation. First, S.B. 1070 is an attempt by Arizona to usurp exclusive federal authority to manage and supervise immigration law enforcement. Second, uniformity in immigration law and immigration law enforcement leaves no place for state laws like S.B. 1070. Third, S.B. 1070 cuts to the core of American freedoms to be free of undue government interference into individuals' daily lives and is manifestly unjust.

a. S.B. 1070 is an improper attempt by Arizona to usurp immigration law, which is the exclusive purview of the federal government.

Immigration law is a field of jurisprudence that is consigned to the federal government to dictate.[33] The Supremacy Clause provides that the "Constitution, and the Laws of the United States which shall be made in Pursuance thereof . . . shall be the supreme Law of the Land."[34] Furthermore, the drafters of the Constitution articulated that immigration and naturalization matters are exclusively vested in the federal government.[35] To this end, the Supreme Court has affirmed that "[t]he authority to control immigration . . . is vested solely in the federal government."[36] Accordingly,

Arizona's attempt to enter the field of immigration is an impermissible act in discord with the United States Constitution and federal law. S.B. 1070 should, therefore, be struck down as unconstitutional.

The Congress has given DHS, and one of its arms, the United States Immigration and Customs Enforcement ("ICE"), authority to operate federal enforcement programs with state and local agencies.[37] This statutory authority includes requirements for local authorities under which they are required to comply in their enforcement of immigration laws. "In S.B. 1070, Arizona has attempted to bypass requirements of ICE supervision and management of its immigration enforcement under a [memorandum of agreement of which Arizona enforcement authorities have entered into]."[38] The American Bar Association most succinctly decried S.B. 1070 when it stated: "[i]n order to maintain uniformity in immigration law and immigration law enforcement, and unless Congress determines to the contrary, a state should not be permitted to usurp federal authority to manage and supervise immigration law enforcement activities."[39]

b. Immigration law requires uniformity and cohesiveness. S.B. 1070 is an impermissible confusion in national policy.

The need for uniformity in national immigration law and its enforcement require a consistent system of jurisprudence that does not vary by state. The Supreme Court has commented on the nature of federal immigration law and its implications in "foreign relations and international commerce."[40] These fragile and significant concerns mandate "delicate policy judgments."[41] Furthermore, the international implications of immigration law vests the federal government with exclusive authority. Finally, the federal government's instituting of immigration law occupies the field and preempts state authority to enact contradictory and even complimentary statutes.

Pursuant to S.B. 1070, state law enforcement officials—a group whose principal concerns relate to public safety and criminal law enforcement—would be called upon to apply and enforce immigration law by establishing the presence of reasonable suspicion and inquiring as to immigration status.[42] However, properly detained individuals under the law may include political or religious asylum seekers coming to America yearning to be free. The effectiveness of state law enforcement in recognizing asylum seekers and coping with such situations in light of the criminal nature of S.B. 1070's provision is unknown.

c. S.B. 1070 is contrary to the United States Constitution, United States laws, and the intrinsic principles upon which the United States was founded.

It is axiomatic under American constitutional provisions and inherent freedoms that an individual should not be subject to undue interference, unfounded accusations, and unreasonable searches. Of course, S.B. 1070 does not permit law enforcement officers from questioning

individuals concerning their immigration status absent reasonable suspicion; however, one does not need a *juris doctorate* in order to perceive the intrinsic proverbial slippery slope upon which this statute stands on the precipice. The subjective reasonable suspicion of one officer is obviously disparate when compared to his colleagues. Moreover, the presumption of appropriateness given to an officer's internal mindset in finding reasonable suspicion is difficult to refute and improper racial animi are difficult to establish.

Application of any criteria for "reasonable suspicion" by its very nature must be subjective. Because of its vagueness, the difficulty in applying any such criteria becomes immediately apparent. Does an Arizona law enforcement official have "reasonable suspicion" to question any individual with dark skin? If so, how dark? Does this apply only to Hispanics or would there be "reasonable suspicion" as to anyone with dark skin such as African-Americans, Indians or even a California Caucasian with a sunburn? Does the fact that a person is not well dressed and is wearing shabby dirty clothes become a further factor in considering whether or not there is "reasonable suspicion." Therefore, are poor people more likely to create reasonable suspicion as compared with well dressed middle class individuals?

Ironically, S.B. 1070 even made it a crime for an illegal immigrant to solicit, apply or perform work. It remains to be seen what would be the *mens rea* of an individual who merely is attempting to find work to raise funds for food and support. No doubt one can argue that if an illegal immigrant provides labor or other services, that work is not available to be undertaken by a valid Arizona resident. Even so, is it appropriate for S.B. 1070 to make it a crime for any individual, even an illegal immigrant, to secure gainful employment? In theory, the harder one works, the greater the magnitude of the crime. This seems to be contrary to the American work ethic.

Moreover, "[o]pponents are particularly concerned about the trespassing provision, stating that it will increase racial profiling. They argue that U.S. citizens and legal immigrants will be approached on the basis of their skin color."[43] Statutes such as S.B. 1070 that are drafted so broadly are assured to ensnare legal American citizens.[44] These opponents further note that state and local officials are poorly trained to handle enforcement of complex federal law.[45] Attempting to refute this assertion, Sheriff Joseph Arpaio of Maricopa County[46] asserts that a two-hour long training class for deputies is wholly sufficient to educate the officers on federal and state immigration law.[47] This is a dubious contention.

Furthermore, the possibility of detention of individuals who are in fact documented citizens but do not have identification is a real concern. According to the ABA and the ACLU, the likelihood of improper arrest due to a lack of documentation is almost assured.[48] According to a 2006 study by the Vera Institute of Justice, 125 individuals in federal immigration detainment facilities were believed to have valid U.S. citizenships but remained in detention due to oversight, electronic errors, or other failings.[49] It has been noted that the federal databases are poorly

integrated, lack complete records, or are flat-out inaccurate.[50] These concerns are material and pose a threat to the freedom of individuals in this country legally and illegally. The concerns and failings of this statute far outweigh any positive remedial effect.

V. Conclusion

With the sour financial condition of the United States combined with the rampant influx of illegal immigrants in border states such as Arizona, it is understood that state legislatures would attempt to stem the tide of low-paid workers who are undercutting many unemployed Americas in garnering jobs. However, S.B. 1070 is the improper mechanism to effectuate this goal. Setting aside the legal argument that the act is an improper attempt to interfere with the exclusive federal prerogative of setting national immigration policy, the statute is manifestly unseemly and is in discord with the tenets of American freedoms. Basic rights to privacy, rights to work, and rights to due process strike against the enforcement of this statute. It is unclear what will occur procedurally as the litigation proceeds through the district court and climbs up the ladder of judicial review to the circuit courts of appeal. Notwithstanding the route this issue takes to final adjudication, one result is proper: S.B. 1070 should be found to be unenforceable as a matter of law.

---

[1] ALEKSANDR SOLZHENITSYN, GULAG ARCHIPELAGO (1973), *available at* http://mitteleuropa.t35.com/wk2_the_gulag_archipelago_01.html (last visited Nov. 15, 2010).

[2] 2010 Ariz. Legis. Serv. Ch. 113 (West 2010).

[3] Rick Su, *The Overlooked Significance of Arizona's New Immigration Law*, 108 MICH. L REV. FIRST IMPRESSIONS 76, 76 (2010).

[4] Miriam Jordan, *Judge Blocks Arizona Law*, WALL ST. J., July 29, 2010, *available at* http://online.wsj.com/article/SB10001424052748703940904575395314079925720.html (last visited Nov. 7, 2010).

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] Pierre Georges Bonnefil, *Understanding the Immigration Debate: An Immediate Look at Arizona's Proposed Immigration Refordm and Federal Government's Response*, Aspatore Spec. Rep., Oct. 2010, at 20.

[10] *Id.*

[11] *Id.*

[12] S.B. 1070, *supra* note 3, at § 1.

[13] Randal C. Archibald, *Arizona Enacts Stringent Law on Immigration*, N.Y. TIMES, April 23, 2010, *available at* http://www.nytimes.com/2010/04/24/us/politics/24immig.html?_r=1 (last visited Nov. 7, 2010).

[14] *Id.*

[15] *Id.*

[16] *Id.* Indeed, the authors' first thoughts of S.B. 1070's provision permitting law enforcement to request immigration documents upon request involved Steve McQueen and his WWII compatriots escaping a German Stalag in *The Great Escape* (1963) and the Gestapo's subsequent demands to produce their "papers."

[17] *Id.*

[18] *See generally* Immigration Nationality Act 8 U.S.C. § 1101 *et seq.* (2010).

[19] Federation for American Immigration Reform, *Support Our Law Enforcement and Safe Neighborhoods Act Summary of Arizona SB 1070 as Enacted*, April 27, 2010, *available at* http://www.fairus.org/site/DocServer/ariz_SB

1070_summary.pdf?docID=4761 (last visited Nov. 7, 2010); *see also* S.B. 1070, *supra* note 3.

[20] *See* United States v. Arizona et al., No. CV 10-1413-PHX-SRB (D. Az. July 28, 2010) (Doc. 87, Order Granting Preliminary Injunction (the "Order")); *see also* Friendly House et al. v. Whiting et al., No. CV10-1061-PHX-SRB (D. Az. July 28, 2010) (Doc. 424, Order)

[21] Order, *supra* note 20.

[22] *Id.*

[23] *Id.*; Bonnefil, *supra* note 9.

[24] Bonnefil, *supra* note 9.

[25] *Id.*

[26] *Id.*

[27] Jordan, *supra* note 4.

[28] *Id.*

[29] *Id.*

[30] As an interesting twist of historical irony, Secretary of Homeland Security Janet Napolitano (D-Az.) is the former governor of Arizona and had vetoed legislation similar to S.B. 1070 on repeated occasions prior to her appointment to her current position by President Obama in 2009.

[31] Jordan, *supra* note 4.

[32] *Id.*

[33] Su, *supra* note 3.

[34] U.S. CONST., art. VI, cl. 2.

[35] U.S. CONST., art. I, § 8, cl. 4.

[36] Traux v. Raich, 239 U.S. 33, 42 (1915).

[37] *See generally* Brief of Amicus Curiae American Bar Association in Support for Preliminary Injunction, Friendly House et al. v. Whiting et al., No. 10-CV-01061-SRB (D. Az. July 14, 2010).

[38] *Id.* at *4.

[39] *Id.* at *6.

[40] Matthews v. Diaz, 426 U.S. 67, 80 (1976).

[41] *Id*.

[42] *See* Brief of Amicus Curiae American Bar Association in Support for Preliminary Injunction, *supra* note 37, at *6-7.

[43] Christina McMahon, *Amidst Controversy Over Federal 287(G) Immigration Program, Arizona Approves Immigration Trespassing Crime Under New Law*, 15 PUB. INT. L. REP. 141, 144 (2010) (internal citations omitted).

[44] *Id.* at 144-45.

[45] *Id*. at 145.

[46] Sheriff Arpaio is perhaps the best known municipal sheriff in the country. Nationally known for requiring county inmates to wear pink colored fatigues as a means of mental punishment, Sheriff Arpaio is an outspoken supporter of S.B. 1070. *See generally*, Natalie Rivers, *Sheriff Arpaio facing lawsuit from immigration activist*, AZFAMILY.COM, Oct. 29, 2010, *available at* http://www.azfamily.com/news/local/Sheriff-Arpaio-facing-lawsuit-from-immigration-activist-106348288.html (last visited Nov. 15, 2010).

[47] McMahon, *supra* note 43, at 145.

[48] *See* Brief of Amicus Curiae American Bar Association in Support for Preliminary Injunction, *supra* note 29, at *7.

[49] *Id.*

[50] *Id.*

Privacy Implications Associated With Medicare Secondary Payer Act and the 2007 Medicare, Medicaid and S-CHIP Extension Act Reporting Requirements

By: Tamela J. White and Allison N. Carroll

THE 2007 Medicare, Medicaid and S-Chip Extension Act (MMSEA)[1] has been the subject of much discussion as the private business sector becomes prepared to meet the obligation to electronically report payments made in civil litigation and other contexts.[2] The MMSEA compliments the Centers for Medicare and Medicaid Services' (CMS) recovery initiatives pursuant to the Medicare Secondary Payer Amendments to the Social Security Act (MSP).[3] The MSP requires any primary payer[4] to be responsible for payment of medically-necessary care. The MSP entitles the United States to recover prior conditional health care payments directly from beneficiaries,[5] primary payers,[6] beneficiaries' attorneys[7] and others.[8]

Since the existence and identity of primary payer sources may be unknown or uncertain at the time health care is provided and payment obligations are incurred, very often Medicare makes payments to health care providers which are deemed conditional and subject to MSP repayment in the event a primary payer source subsequently acknowledges and pays for the subject medically-necessary care. As the federal government has improved its computer networking interoperability, and its capacity to track and mandate conditional payment, repayment compliance has increased. With adoption of the Medicare, Medicaid S-CHIP Extension Act, CMS and OIG (the Office of Inspector General) anticipate a greater repayment recovery of prior conditional payments made.[9]

The MMSEA's mandates implicate privacy issues because they require MMSEA reporting entities to obtain and report individually identifiable, personal information. Each primary payer must designate a Registered Responsible Entity (RRE)[10] that must register with CMS for reporting purposes.[11] Each RRE must populate CMS data fields with specific, personal, individual, identifiable information into CMS' secure computer

Ms. White is a Member of Farrell, Farrell & Farrell, PLLC. A former critical care nurse and hospital administrator, Ms. White practices in Huntington West Virginia. She will receive her Masters' in Public Health from the Johns Hopkins Bloomberg School of Public Health in 2011. Ms. White's practice includes health law and regulation, medical defense and litigation in the fields of product liability, health law and medical negligence.

Ms. Carroll is an associate with Farrell, Farrell & Farrell, PLLC. She received her law degree, cum laude, from the Louis D. Brandeis School of Law at the University of Louisville in 2006. Her practice includes medical defense and litigation in the areas of product liability, health law and medical negligence.

data base. For each individual, this includes name (and any former names or derivations of the same), address, sex, social security number or Health Identification Claim Number (HICN) and at least one ICD-9 code.[12]

The RRE, who may be the primary payer or an entity contracted to provide this service for a primary payer,[13] has the obligation to report payments to beneficiaries, agreed upon generally through a contract of insurance, settlement agreement or judgment.[14] The primary payer does not have the fiduciary duty to maximize recovery for the beneficiary. The beneficiary's interests often are protected through counsel whose duties include zealous representation and maximization of the final dollar amount realized by the client beneficiary. RREs, the primary payer plan(s), and its/their respective counsel, each have separate and distinct duties to preserve and represent their respective interests and not necessarily to maximize a beneficiary's personal recovery. For instance, with respect to the MMSEA specifically, RREs and primary plans have the highly-motivating self interest to avoid the $1,000 per day "late claim" reporting sanction and liability for double damages in the event of a failure to timely report a payment or an ongoing payment obligation.[15]

In this electronic generation, identity theft and misuse or misappropriation of personal identifiers is a substantial problem and concern. Identity theft is one of the "fastest growing crimes in America."[16] Health (medical) identity theft is such an increasing concern that the Office of the National Coordinator for Health Information Technology (ONCHIT) published a final report, on January 15, 2009, outlining numerous interventions it deemed to be necessary to protect individual health identity.[17] Health (medical) identity theft happens when a person uses another person's name and some other unique individual identifier, such as insurance information, a social security number, or an HICN for the purpose of obtaining medical goods or services or to obtain money by falsifying medical services claims.[18] The essence of this crime is the use of the medical identity of another without knowledge of the person whose information is being used.[19]

The statistical summaries of health identity theft are mere estimates and are believed to underestimate the scope of the problem.[20] Identity theft reports, not specific to health/medical identity, have risen yearly since data on this broad category of crimes has been collected. For instance, in 2001 the number of persons reporting identity theft was 86,168 and in 2005, this number was 255,565.[21] The Social Security Administration, Office of Inspector General's beneficiary hotline has reported that from March through September 2001, it received 25,991 identity theft reports with 548 of these including allegations of medical identity theft.[22]

Substantial resources are spent each year in the private and public sectors attempting to prevent inadvertent publication of individual identifiers and misappropriation of confidential information. A Privacy Impact Assessment (PIA) is required by each governmental agency, pursuant to Titles II and III of the E-Government Act of 2002.[23] A PIA was been completed by

the United States Office of Personnel Management concerning the Medicare Secondary Payer System (MSPS) as of September 7, 2007.[24] However, this PIA was prepared before release of any proposed MMSEA enforcement regulations or guidelines and the mandatory MSP data reporting system.

Primary payer plans and RREs generally have established compliance programs which safeguard dissemination of private health information and unique personal identifiers. The phrase "Zero Tolerance" is commonplace in industry jargon. The Privacy Act of 1974,[25] the Health Insurance Portability and Accountability Act of 1996[26] with corresponding Privacy Standards,[27] and other laws, such as state insurance department regulations, provide a complex framework designed to protect the individual's privacy interests.[28]

Notwithstanding these facts, as MSP recovery efforts intensify and the MMSEA electronic data reporting becomes a reality[29] discovery disputes will arise in the trenches. There are two published opinions from 2010 discussed herein, in which trial courts addressed settlement and discovery issues arising out of the MMSEA and the MSP: *Hackley, et al. v. Garofano, et al.*[30] and *Seger v. Tank Connection, LLC., et al.*[31] Each is instructive in providing guidance in those domains. Primary payer (insurer and RRE class) electronic storage and retention of personally identifiable health information was opposed by a plaintiff in *State Farm Mutual Automobile Insurance Company v. Bedell.*[32] That decision, while having no MSP/MMSEA issue before it, is a good example of how counsel must consider competing legal obligations governing privacy and other interests which may arise.

This article provides a brief overview of the MMSEA Reporting Obligations, followed by a discussion of these opinions and the privacy and ethical issues presented in them concerning exchange of social security number, HICN and ICD-9 Code designation required by compliance with the MMSEA.

I. Brief Overview of the MMSEA Reporting Obligations

The MMSEA requires an RRE to report "claims" to CMS through its Coordination of Benefits Contractor (COBC). A "claim" is the overall claim for liability insurance (including self-insurance), no-fault insurance or workers' compensation rather than a single claim for a particular medical item or service.[33] Claim information relates to a primary plan's payment to a Medicare beneficiary where the beneficiary claims medical damages which are released or satisfied by settlement, judgment, award or otherwise.[34] Each RRE must register with its designated COBC and must designate a responsible authorized representative,[35] an authorized account manager,[36] and account designees[37] for compliance purposes.

RREs must register with CMS' secure user electronic reporting data bank.[38] It is CMS' intention that once an RRE is registered, it will be assigned a quarterly reporting schedule for Claim Input File Submission. The quarterly data input period assigned to each RRE is limited to a 7-day window.[39] Access to the portal is closed to the RRE for

reporting purposes. However, the RRE may query the data bank at any time as to whether a claimant is a beneficiary, by inputting name, sex, date of birth, and either the social security number or HICN.[40] Social security numbers or HICNs drive the identity confirmation since it is through these unique personal identifiers that CMS manages the benefits provided to individuals. Many primary plans and RREs will rely upon the query process to document their attempt to determine, through CMS itself, whether an individual claimant is a beneficiary for MSP purposes.

II. *Hackley, et al. v. Garofano, et al.,*[41] *Seger v. Tank Connection, LLC., et al.*[42] and *State Farm Mutual Automobile Insurance Company v. Bedell*[43]

In *Hackley, et al. v. Garafano, et al,* the Connecticut Superior Court concluded that there had been no meeting of the minds and refused to enforce a settlement when, after the settlement amount had been agreed upon by the parties, the plaintiffs objected to the insurer's request for their social security numbers. Importantly, the Court found that the insurer could have made disclosure of social security numbers, even for a minor plaintiff and non-Medicare beneficiary, a pre-condition to settlement but, its having failed to do so, there was no enforceable agreement. [44]

The underlying facts were as follows. The minor plaintiff was injured in a motor vehicle accident on July 1, 2007, and was still a minor at the time his father attempted settlement with the insurer, USAA. The monetary sum of $7,500.00 was agreed upon to settle the claim. After that agreement was reached, USAA requested the social security number of both the minor and father. The plaintiffs refused on the basis that the requested information was confidential, the son was a minor and obviously was not Medicare eligible, and the father's social security information was not relevant.

The Court recognized the MSP obligations and concerns asserted by the insurer. Since the insurer had failed to specifically include the demand for release of social security numbers in the settlement negotiations, the court refused to enforce the settlement. In recognition of the consequences for failed MSP reporting, the Court affirmed an insurer's right to condition a settlement upon the provision of social security numbers to be used for CMS MMSEA querying and reporting. The Court rejected plaintiffs' arguments that the minor plaintiff was not Medicare eligible and also found that the father's social security number could be demanded since the MMSEA "affect[s] *all* parties involved in a payment of a settlement, judgment or award."[45] The Courts' conclusion bears a reminder for all participants in these discussions:

> This is hardly the first settlement to be derailed because of unresolved questions relating to Medicare liens. Rarely, these have led to published decisions. See, e.g., *Riccardi v. Strunk,* Judicial District [Initial caps needed?] of New London, Docket No. CV 08 5008671 (January 22, 2010, Cosgrove, J.). More frequently, they have simply led to frustration and misunderstanding. Counsel would therefore be well

> advised to be aware of developments in this area of law and take them into account in fashioning unambiguous settlement agreements.[46]

Therefore, when preparing for a mediation or settlement conference, as well as in the negotiation of the terms of any settlement, parties should include mandatory MSP/MMSEA compliance data and include as a material term in the settlement documents, confirmation of the accuracy of all such data uniquely in the possession of the beneficiary and his or her counsel.

Seger v. Tank Connection, LLC[47] involved a discovery dispute. Interrogatories were sent to plaintiff requesting the specific information required to populate the CMS data bank reporting fields, including the plaintiff's social security number. The requesting party based its request upon MMSEA compliance mandates, asserting *inter alia* that it may be impossible to obtain the requested information after a settlement, judgment or finding of liability because plaintiff would have no incentive to provide the information at those times.[48] Plaintiff objected on grounds that the information was irrelevant, immaterial and not likely to lead to the discovery of admissible evidence. Plaintiff argued that no mandatory reporting obligation existed unless liability was accepted and that the requested information would be provided "within a time specified by the Secretary [of the Department of Health and Human Services] after the claim is resolved through a settlement, judgment, award or other payment (regardless of whether or not there is a determination or admission of liability)."[49]

The Court found that the MSP/MMSEA reporting mandates controlled and it ordered the plaintiff to respond to the discovery. The Court found that there was no harm in providing the information before settlement or judgment. However, the Court did not agree with the defendant's position that MMSEA compliance information was necessary in order to negotiate a settlement, implying that this information was available through alternative means including medical records relied upon in the case. The Court ultimately concluded that the requested information would have to be provided at some point in time and that the discovery was proper, requiring Rule 26 compliance by the plaintiff in responding.[50]

An important issue not discussed in the *Seger* decision is whether a protective order is warranted prior to a plaintiff responding to interrogatory or deposition questioning intended for MSP/MMSEA compliance. By way of example, a typical set of discovery may include:

> For purposes of mandatory compliance with the Medicare Secondary Payer Act, the Medicare, Medicaid and SCHIP extension act of 2007 or any private contractual subrogor, provide each name by which _____ has ever been known, his date of birth, his social security number, the date(s) (if any) that he qualified for Medicare, the date(s) (if any) that he became a Medicare beneficiary, his Health Identification Claim Number (HICN), each ICD-9 diagnostic code relating to the claimed injury for which recovery is sought in this

> case, whether or not the appropriate Medicare benefits coordinator has been contacted regarding this civil action and whether or not Medicare has notified you that it seeks conditional medical expense payment reimbursement from any recovery in this action.
>
> Please state whether _____ had, at any time prior to his death, been a Medicare beneficiary by virtue of end stage renal disease and/or disability of any kind.
>
> Please produce all notices of claim of any nature from any governmental or third party entity asserting a right to repayment of prior medical payments made arising out of the injuries for which recovery is sought in this matter.
>
> Please produce all notices by you or on your behalf to and/or from the Centers for Medicare and Medicaid Services (COBC) concerning your attempt to recover damages arising out of the health care expenses incurred for which recovery is sought in this matter.

Each of these sample requests is specific to MSP/MMSEA compliance and liability issues. Whether requesting counsel should preempt delay by proposing a protective order governing dissemination of this information is for evaluation with his/her client and responsible primary plan representatives.

The issue of protective orders governing personally identifiable information was addressed *State Farm Mutual Automobile Insurance Company v. Bedell.*[51] This case did not involve MSP or MMSEA construction. However, the issue presented was and is a foreseeable one for future MSP/MMSEA claims management.

The plaintiff in *Bedel* was injured in an automobile accident. During the discovery phase of the litigation, plaintiff objected to production of health information absent a protective order requiring that the defendants' insurer to abstain from electronic storage of private health information and to return or destroy disclosed information at the conclusion of the case. The trial court entered a protective order, over the objection of the defendants, requiring, in relevant part:

> Defendants' counsel will not disclose orally or in summary form, any of the Plaintiff's or Decedent's medical records, or medical information, to any person other… than their clients, office staff, and experts necessary to assist in this case, and any such person shall be advised of this Protective Order and receive and review a copy of it and be informed that they are bound by the non-disclosure terms and the other provisions of this Protective Order if they receive such protected information. *No person shall scan or store any of Plaintiff's or the Decedent's medical records or medical information by any method,* including but not limited to, computerized storage, filming, photographing, microfiche or other similar method….
>
> Also, upon conclusion of this case, all medical records, and medical information, or any copies

> or summaries thereof, will either be destroyed with a certificate from Defendants' counsel as an officer of the Court that the same has been done, or all such material will be returned to Plaintiff's counsel without retention by Defendants' counsel or any other person who was furnished such materials and information pursuant to the terms of this Protective Order. Provided however should Defendants' counsel desire to retain a copy of the protested [sic] medical records produced in this case, the same shall be permitted as long as those protected medical records are maintained in a sealed manner in Defense Counsel's file and not used for any other purpose whatsoever except upon further order of this Court or in response to lawful process after notice to the protected person, or in response to a lawful order of another Court with jurisdiction, or upon written consent of the protected person whose medical records and information is protected herein.[52]

State Farm relied principally upon the records retention requirements of the West Virginia Insurance Commissioner in asserting its objections. Those record retention requirements included, *inter alia*, confidentiality obligations, storage obligations, electronic storage options, and a mandatory retention period.

The *Bedel* Court declared the protective order to be improper, relying upon the state insurance commissioner's rules and regulations.[53] Specifically, the Court found:

> To further protect the confidentiality of an insured's medical records, the Insurance Commissioner has promulgated a legislative rule, W. Va.C.S.R. § 114-57-15 (2002), based on the model privacy rules of the National Association of Insurance Commissioners, which are patterned after the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2009), *et seq.* Among other things, this rule prohibits insurers from disclosing 'nonpublic personal health information' without authorization by the individual. W. Va.C.S.R. § 114-57-15.1. Thus, insurers operating in West Virginia are required to prevent the unauthorized disclosure of confidential medical records contained in claim files, whether those files are stored electronically or in paper format.[54]

As MSP/MMSEA challenges materialize in the future, counsel should consider these collateral sources of confidentiality protection in fashioning a means by which to accomplish that which all participants in the dispute need: exchange of information in the least restrictive and yet protective manner respectful of the privacy of the beneficiary.

III. Discussion

These three decisions prompt a robust privacy discussion. The MSP preempts state law.[55] To the extent that

state law conflicts with MSP enforcement, courts have found that the federal information recovery mandates are superior.[56] Further, the filing of a Medicare claim by or on behalf of a beneficiary is an express authorization by the beneficiary for "any entity, including State Medicaid and workers' compensation agencies and data depositories" to release information concerning the subject claim to CMS for MMSEA enforcement.[57]

An underlying apparent assumption was made in *Hackley* that the absence of Medicare age qualifying status , end-stage renal disease, or dual eligibility is not a basis for a plaintiff to object to a primary payer's protection of its interests by conditioning settlement upon release of otherwise protected information. However, the settlement phase of a claim or litigated case is late in the process for both plaintiffs' and defendants' counsel to be thinking about the subrogation interests of third parties, including the government. Counsel should be willing to respect the obligations of all participants in pre-litigation and discovery. By application of a primary payer's own compliance programs, operation of state law, and conformity with federal privacy standards and requirements, appropriately tailored protective orders and discovery guidelines should be attainable by agreement between the parties.

Emphasis thus far in this article has been upon social security number and HICN disclosure. An additional and significant MMSEA disclosure mandate warrants special consideration: the International Classification of Diseases (ICD) disclosure mandate. The ICD is:

> the international standard diagnostic classification for all general epidemiological [and] many health management purposes and clinical use. These include the analysis of the general health situation of population groups and monitoring of the incidence and prevalence of diseases and other health problems in relation to other variables such as the characteristics and circumstances of the individuals affected, reimbursement, resource allocation, quality and guidelines. It is used to classify diseases and other health problems recorded on many types of health and vital records including death certificates and health records. In addition to enabling the storage and retrieval of diagnostic information for clinical, epidemiological and quality purposes, these records also provide the basis for the compilation of national mortality and morbidity statistics by WHO Member States. [58]

In simple terms, the ICD code drives reimbursement and with respect to government health care payments, it drives CMS' assessment of disease states for which a beneficiary has received treatment. The consequences of a primary payer or RRE populating a mandatory CMS MMSEA data field with the wrong ICD are self apparent. For example:

> ICD-9-CM codes do not differentiate between right and left appendages. Thus, report of an ICD-9-CM code for a left ankle injury incurred in a car accident may cause Medicare to

> include in its claim medical bills Medicare paid for an injury to the claimant's right ankle. This can, in turn, cause CMS to grossly overestimate the total amount owed, leaving a disparity between what the RRE reports and what CMS expects.[59]

If the wrong ICD is used, a beneficiary may sustain compromised benefits. If a beneficiary's attorney is not careful and includes in a demand the ICD coding for numerous unrelated conditions or expenses, the attorney may be unable to maximize his or her client's realized recovery. Stated simply, asking for more than reasonably arises out of the alleged dispute may result in adverse consequences for the injured party. Likewise, if the beneficiary and his or her counsel refuse to identify the appropriate ICD code prior to mandatory reporting, a RRE may have no other choice but to populate the CMS data bank fields with all ICDs listed on a claimant's bills. Any negotiating RRE, primary plan or primary plan counsel must include express ICD designation as a pre-condition to settlement. Those ICD designations must match the subject matter in the litigation with all parties recognizing that the ultimate determination of that which constitutes a prior conditional payment being the discretion of CMS. This emphasizes the obligation that counsel representing the beneficiary should cooperatively work with CMS to define the ICD code(s) related to the lawsuit.

These and other significant privacy concerns must be anticipated and managed in a proactive manner. This field will continue to evolve in the foreseeable future. For instance, on March 9, 2010, United States Representative Patrick Murphy introduced the "Medicare Secondary Payer Enhancement Act of 2010" (MSPEA).[60] Section 4 of the Bill proposes the adoption of safe harbors with respect to the MMSEA reporting obligations and restructures the penalty obligations for late reporting based upon intent. Section 5 provides that "the Secretary [of the Department of Health and Human Services] shall modify the reporting requirements . . . so that entities responsible for reporting information . . . are not required to access or report to the Secretary beneficiary social security numbers or health identification claim numbers."[61] Whether this bill will be acted upon soon or gains material traction is to be seen. It does not, however address ICD information. It also does nothing to relieve the present obligations under existing regulations. The next chapters in this saga will take some time to work out. Hence, as the *Hackley* court admonished, "[c]ounsel would therefore be well advised to be aware of developments in this area of law and take them into account in fashioning unambiguous settlement agreements."[62]

---

[1] Medicare, Medicaid, and SCHIP Extension Act of 2007, Pub. L. No. 110-173, 121 Stat. 2492 (2007).

[2] *See, e.g.*, OIG 2011 Work Plan, Longstanding Issues, Recovery Act Reviews Among Areas of Focus, 20 No. 3 HTHCR 6, Aspen Publishers 2010; Jason D. Lazarus, *Medicare Myths: What Every Trial Lawyer Should Know About the MSP*

& Liability Medicare Set Asides, 84NOV FLA. B.J. 46 (November, 2010); Brent M. Timberlake and Monica A. Stahly, *Fool Me Once, Shame on Me; Fool Me Again and You're Gonna Pay For It: An Analysis Of Medicare's New Reporting Requirements For Primary Payers And The Stiff Penalties Associated With Noncompliance*, 45 U. RICH. L. REV. 119 (2010); Frederick C. Geilfuss, B. McGrath and M. Kwiecinski, *Reporting Risk Management Activities to CMS Under the MMSEA: Hospitals, Physicians and Provides Need to Become Familiar with New Guidance*, 12 No. 5 J. HEALTH CARE COMPLIANCE 53 (September/October 2010); Tamela J. White, *The Medicare Secondary Payer Act and Section 111 of the Medicare, Medicaid, SCHIP Extension Act of 2007: Implications for Claim Management and Resolution for Liability Insurance Plans*, 77 DEF. COUNS. J. 157 (2010).

[3] 42 U.S.C.1395y(b) (2010).

[4] Primary payer means, "when used in the context in which Medicare is the secondary payer, any entity that is or was required or responsible to make payment with respect to an item or service (or any portion thereof) under a primary plan. These entities include, but are not limited to, insurers or self-insurers, third party administrators, and all employers that sponsor or contribute to group health plans or large group health plans." 42 C.F.R. §411.21(2008).

[5] Medicare beneficiary means an individual who is entitled to or enrolled in Medicare Part A (Hospital Insurance) or enrolled in Part B (Supplementary Medical Insurance) or both under title XVIII of the Act. 20 C.F.R. §418.3010(b)(8)(2005). 42 C. F. R. 411.24(h) (2008) requires a beneficiary "or other party" that receives a primary payment to reimburse Medicare within 60 days. Failure to repay promptly may compromise a beneficiary's status and CMS may require the beneficiary to make payment, with interest. United States v. Harris, No. 5:08CV102, 2009 WL 891931 (N.D. W. Va. Mar. 26, 2009), *aff'd*, 334 Fed. Appx. 569 (4th Cir. 2009).

[6] *See supra* note 5; 42 C.F.R. § 411.21 (2008).

[7] United States v. Harris, No. 5:08CV102, 2009 WL 891931 (N.D. W. Va. Mar. 26, 2009), *aff'd*, 334 Fed. Appx. 569 (4th Cir. 2009).

[8] MSP obligations exist for employers, workers' compensation plans, group health plans and others. *See supra* note 5; 42 C.F.R. § 411.21 (2008).

[9] *See* OIG 211 Work Plan, Longstanding Issues, Recovery Act Reviews Among Areas of Focus, 20 No. 3 HHTHCR 6, Aspen Publishers, 2010.

[10] RREs are those entities responsible for complying with the reporting requirements of MMSEA Section 111. *See* MMSEA User Guide, at 9, 21 ("42 U.S.C. 1395y(b)(8)(2010) provides that the 'applicable plan' is the RRE and defines 'applicable plan' as… 'the following laws, plans, or other arrangements, including the fiduciary or administrator for such law, plan, or arrangement: (i) liability insurance (including self-insurance); (ii) no-fault insurance; (iii) Workers' compensation laws or plans.'").

[11] CMS, *MMSEA Section 111 Medicare Secondary Payer Mandatory Reporting: Liability Insurance (Including Self-Insurance), No-Fault Insurance, and Workers' Compensation USER GUIDE* (hereinafter "MMSEA User Guide"), Version 3.1, July 12, 2010, at 18.

[12] MMSEA User Guide, *supra* note 11 at Appendix A (setting forth the complete list of fields which must be populated when reporting a claims pursuant to MMSEA Section 111).

[13] MMSEA User Guide, *supra* note 11 at 21-29 ("Agents are not RREs for purposes of the MSP reporting responsibilities for 42 U.S.C. 1395y(b)(7). However, the

applicable RRE may contract with an entity to act as an agent for reporting purposes.").

[14] *See* 42 C.F.R. §411.210(2008) ("Primary payment means, when used in the context in which Medicare is the secondary payer, payment by a primary payer for services that are also covered under Medicare.")

[15] 42 U.S.C. §1395y(b)(2)(B)(ii)(2010).

[16] Social Security Administration, http://www.ssa.gov/pubs/10064.html (last accessed Dec. 10, 2010).

[17] United States Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Medical Identity Theft Final Report, January 15, 2009, Prepared by Booz Allen Hamilton.

[18] The World Privacy Forum, *Medical Identity Theft: The Information Crime That Can Kill You*. Spring, 2006. Available at http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006 (last accessed Dec. 10, 2010).

[19] *Id*. at 16.

[20] *Id*. at. 20.

[21] *Id*. (reporting information received from the Federal Trade Commission pursuant to a FOIA request, FTC FOIA-2006-00560).

[22] *Id*. at 21.

[23] 42 U.S.C. §101 (2002), *et seq*.

[24] Medicare Primary Payer System (MSPA) Privacy Impact Assessment, United States Office of Personnel Management, Available at http://www.opm.gov/privacy/PIAs/pia_msps.asp (last accessed December 10, 2010).

[25] 5 U.S.C. §552a (2010).

[26] Pub. L. No. 104-191, 110 Stat. 1936 to 1996 (codified at 29 U.S.C. 1162(2)(A)(v)(2000)).

[27] 45 C.F.R. pts. 160, 162, 164.

[28] *See generally*, 50 STATE STATUTORY SURVEYS, INSURANCE GENERAL, Thomson Reuters/West December 2009.

[29] The required submission of liability insurance (including self-insurance) initial claim reports was initially scheduled to begin during the first calendar quarter of 2011. The compliance date has now been moved to the first calendar quarter of 2012 for all liability insurance (including self-insurance) TPOC (Total Payment Obligation to the Claimant) amounts with no ORM (Ongoing Responsibility for Medical Payment). *Revised Implementation Timeline for TPOC Liability Insurance (Including Self-Insurance) Settlements, Judgments, Awards or Other Payments*, Alert from the Centers for Medicare & Medicaid Services Office of Financial Management/Financial Services Group, November 9, 2010. Liability insurance (including self-insurance) ORM reporting is not subject to this delay, therefore, reporting begins on January 1, 2011, as scheduled.

[30] 2010 WL 3025597 (Conn. Super. July 1, 2010).

[31] 2010 WL 1665253 (D. Neb. April 22, 2010).

[32] 226 W.Va. 138, 697 S.E.2d 730 (2010).

[33] MMSEA User Guide, *supra* note 11 at 18.

[34] MMSEA User Guide, *supra* note 11 at 18.

[35] The authorized representative is the person with legal authority to bind the plan entity and has ultimate compliance accountability. The authorized representative may assist in registration of an entity but is not issued an account Login ID or password and cannot be an account user or agent. The authorized representative is responsible to designate the account manager. The authorized representative must approve the account profile setup and is the agent for service of non-compliance notifications. MMSEA User Guide, *supra* note 11 at 31.

[36] The account manager controls the RRE account administration and reporting process. The account manager is responsible for web-access registration and account setup. Persons reporting to the account manager, known as "account designees" are provided authorized reporting access once invited by the account manager. The account manager oversees

the logistics of information transfer to the COBC. The manager can monitor RRE usage activities, such as file transmission histories, processing status, and file statistics. The account manager cannot also serve as the authorized representative or as an account designee for the same RRE ID. MMSEA User Guide, *supra* note 11 at 31-32.

[37] Account designees are essentially the data processing personnel that input data into the electronic system. Account designees cannot serve as an account manager or authorized representative. MMSEA User Guide, *supra* note 11 at 31-32.

[38] The portal for the data bank entry is at www.Section111.cms.hhs.gov.

[39] MMSEA User Guide, *supra* note 11 at 44.

[40] MMSEA User Guide, *supra* note 11 at 110.

[41] 2010 WL 3025597 (Conn. Super. July 1, 2010).

[42] 2010 WL 1665253 (D. Neb. April 22, 2010).

[43] 226 W.Va. 138, 697 S.E.2d 730 (2010).

[44] 2010 WL 3025597, at *5-6 (Conn. Super. July 1, 2010).

[45] *Id*. at *4 (Conn. Super. July 1, 2010).

[46] *Id*. at *6 (Conn. Super. July 1, 2010).

[47] 2010 WL 1665253 (D. Neb. April 22, 2010).

[48] *Id*. at *2 (D. Neb. April 22, 2010).

[49] *Id*. at *3 (D. Neb. April 22, 2010).

[50] *Id*. at *6 (D. Neb. April 22, 2010).

[51] 226 W.Va. 138, 697 S.E.2d 730 (2010).

[52] *Id*. at 734 (emphasis in original).

[53] *Id*. at 740.

[54] *Id*. at 738.

[55] Zinman v. Shalala, 67 F.3d 841, 845 (9th Cir. 1995); *see also* English v. Gen. Elec. Co., 496 U.S. 72, 79 (1990); Pac. Gas & Elec. Co. v. State Energy Res. Conservation and Dev. Comm'n, 461 U.S. 190, 204 (1983); United States v. R.I. Insurer's Insolvency Fund, 80 F.3d 616 (1st Cir. 1996)(state laws designed to protect private interests in the event of liability insurance carrier insolvency are preempted by the MSP, as are any state laws that otherwise interfere with federal recovery); Cox v. Shalala, 112 F.3d 151 (4th Cir. 1997) (federal law pre-empted the North Carolina wrongful death act which placed a $1,500.00 cap on third party recovery of medical expenses; Medicare entitled to recover the $181,187.75 that it conditionally paid when the parties to the wrongful death action settled the matter (citing Fla. Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 142, 142-43 (1963)); State Farm v. State of California, ___ F. Supp. ___ (C.D. Calif. 1997) (memorandum opinion) (Medicare entitled to recover the entire settlement res where its conditional payments exceeded the paying automobile insurer's policy limits).

[56] *See supra* note 55.

[57] 42 C.F.R. §411.24(a)(2006).

[58] World Health Organization, International Classification of Diseases definition, available at http://www.who.int/classifications/icd/en/index.html (last accessed December 10, 2010).

[59] Timberlake and Stahly, 45 U. RICH. L. REV. at 119 (internal citations omitted).

[60] Medicare Secondary Payer Enhancement Act of 2010, H.R. 4796, 111th Congress.

[61] *Id.*

[62] 2010 WL 3025597 * at 6 (Conn. Super. July 1, 2010).

Privacy Breach Notification under Canadian Privacy Law – Case Studies for Understanding an Emerging Regime

By John P. Beardwood and Gabriel M. A. Stern

CANADA has one of the world's most comprehensive legal regimes for protecting personal information. This regime covers both the private and public sectors and is largely the result of detailed legislation[1] in force across the country, which sets out rules for how personal information can be collected, used and disclosed. Notwithstanding the scope of this regime, one long-standing gap has been in respect of establishing what obligations organizations have when there has been a personal information breach. In 2010, however, certain legislative amendments were made and proposed that established breach notification obligations. These legislative amendments promise to introduce new challenges for organizations as they seek to comply with Canadian privacy law.

In order to assist counsel in understanding these new and pending Canadian privacy breach notification obligations, this paper (a) introduces the Canadian privacy regime generally, (b) outlines the new Canadian breach notification rules, and (c) reviews three breach notification scenarios in order to illustrate the considerations organizations will need to address in complying with this new and developing regime.

John P. Beardwood is a partner and Gabriel M. A. Stern is an associate at the Toronto office of Fasken Martineau DuMoulin LLP.

I. The Canadian Privacy Regime Generally

A. Structure of the Canadian Privacy Regime

The Canadian privacy law regime is characterized by both federal and provincial[2] privacy legislation, in both the public and private sectors. In the private sector, which is the focus of this paper[3], the application of these laws to different organizations depends on (a) the nature of the organization, (b) the type of activities carried out by the organization, and (c) the places of activity of the organization. On a general level, the basic structure of the Canadian privacy law regime is that the federal private sector privacy legislation - the Personal Information Protection and Electronic Documents Act ("**PIPEDA**")[4] – protects personal information collected, used or disclosed (a) by all federal works, undertakings and business[5], and (b) in connection with the commercial activities of all private sector organizations across Canada, unless a particular province has in force provincial privacy legislation that is deemed "substantially similar" to the federal legislation[6]; in this sense it is

"gap-filling" legislation. In contrast, each of the provincial privacy legislation applies to the activities of all private sector organizations in that province. . Since PIPEDA has been enacted, legislation in the provinces of Quebec[7], British Columbia[8] and Alberta[9] (the "**Alberta PIPA**") has been deemed "substantially similar". As a result, PIPEDA only applies in those three provinces to the collections, uses and disclosures of personal information where conducted by a federal work, undertaking or business, or where disclosed outside the province for a commercial purpose. At both the federal and provincial levels, privacy commissioners are appointed to oversee and enforce privacy legislation.

B. Application Outside of Canada

It is significant to note that the Canadian privacy law regime does not apply only to Canadian organizations but also to any organization carrying on business in Canada, even if they do not have a physical presence in the country. This point was explicitly made in respect of the Federal Privacy Commissioner and the scope of her jurisdiction in 2007 when the Federal Court of Canada confirmed that the federal privacy commissioner (the "**Federal Commissioner**") had jurisdiction to investigate cross-border flows of personal information, even when the organization it was investigating was not located in Canada such that enforcement might be difficult[10].

In 2010, significant amendments were, respectively, made to the Alberta PIPA and proposed to be made to PIPEDA concerning the notification that must be made when there are breaches of organizations' privacy obligations. The amendments, which are described in detail below, are the first in Canada to deal with breach notification and are the focus of this paper.

C. Definition of Personal Information

PIPEDA broadly defines "personal information" as "information about an identifiable person," but excludes the name, title or business address or telephone number of an employee of an organization[11]. The provincial legislation generally includes similar definitions – for example, the Alberta PIPA[12] contains a similar definition, but excludes a broader range of business contact information than PIPEDA by additionally excluding business email and facsimile numbers[13].

II. Privacy Breach Notification Requirements

A. Comparing the Federal and Alberta Models Generally

In the spring of 2010, in respect of breach notification (a) the Alberta PIPA was significantly amended as a result of important amendments that came into force on May 1, 2010, and (b) significant amendments were proposed for PIPEDA on May 25, 2010, pursuant to Bills C-28 and C-29[14].

Under the proposed PIPEDA amendments, a new Division 1.1 will require organizations (a) to report to the Federal Privacy Commissioner any material breach, as defined in PIPEDA, of security safeguards involving any

personal information under that organization's control, and (b) to notify individuals of such breaches where it is reasonable under the circumstances to believe that the breach creates a real risk of "significant harm" (as defined in PIPEDA) to the individual. Along with defining the thresholds for when such breaches will impose the obligations to report these breaches to the Federal Commissioner and/or notify the subject individuals, Division 1.1 also sets out details as to the timing for such notification and the form in which it must be provided.

Similar to what has been introduced by the proposed revisions to PIPEDA, the amended Alberta PIPA introduces both a reporting and a notification regime in respect of security breaches. Under this regime, certain privacy breaches must be reported to the Alberta privacy commissioner (the "**Alberta Commissioner**"), and under very similar circumstances affected individuals must notified of such breaches.

While the federal and Alberta breach notification models may appear somewhat similar at first glance, they differ in five significant ways: (a) the threshold for reporting a breach, (b) the threshold for notifying the affected to individuals, (c) the definition of "significant harm", (d) the responsibility for notification, and (e) offences.

B. Threshold for Reporting a Breach

Under the proposed PIPEDA breach notification model, the threshold for when a breach needs to be reported to the Federal Commissioner is a contextual threshold, which arguably allows for more flexibility as it will better reflect the differing circumstances of each breach. The proposed test for this threshold is, objectively, a "*material breach of security safeguards*", where relevant factors include (a) the sensitivity of the personal information in question, (b) the number of individuals, and (c) a subjective assessment of the organization as to whether reflective of systemic problems.

In contrast, under the Alberta PIPA, the threshold for reporting breaches to the Alberta Commissioner is both significantly lower (in that there may only be one individual involved) and significantly higher (in that breaches of low sensitivity information, which are either frequent, or involve a large number of individuals, are effectively excluded from the reporting requirement). The applicable test is whether, objectively, "*a reasonable person would consider that there is a real risk of significant harm to an individua*l".

C. Threshold for Notifying the Affected Individuals

The proposed test under PIPEDA for when organizations would need to notify individuals that there has been a breach of their personal information is an objective test that considers whether it is "reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual".

The comparable test under the Alberta PIPA is also objective and requires organizations to "*notify individuals to whom there is a real risk of significant harm*". Interestingly, this test

is almost identical to the Alberta PIPAs reporting test discussed above. The significant difference is that the reference to "reasonable person" contained in the Alberta test for reporting is deleted. It is unclear whether this deletion was intentional[15] and what will be the result of this missing language.

D. Definition of "Significant Harm"

The proposed definition for "significant harm" under PIPEDA includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property." Interestingly, the PIPEDA definition appears to effectively deem all of the above kinds of harm as being "significant", while in fact "damage to relationships", "loss of business or professional opportunities" and "damage to or loss of property", for example, may not – depending on the context – be significant. Additionally, identifying whether there is a "real risk of significant harm" includes a review of the following relevant factors: sensitivity of the personal information; and probability (i.e. risk) of misuse. In short, the applicable equation under PIPEDA will be sensitivity of info + probability = harm; plus an evaluation as to whether the harm is significant.

Under the Alberta PIPA, "significant harm" and "real risk" are not defined. Note however that a publication from the Alberta Commissioner[16] ("**Alberta Information Sheet 11**") provides the following definitional guidance, which is more general – and our view therefore more helpful - than the proposed PIPEDA definitions:

(a) "significant harm" is "material harm", having "non-trivial consequences or effects". Examples: may include "possible" "financial loss, identity theft, physical harm, humiliation to one's professional or personal reputation". This test is objective – therefore one does not need to assess the subjective circumstances of the particular individual; and

(b) "real risk": a "reasonable degree of likelihood that the harm could result". Note that "[t]he risk of harm is not hypothetical or theoretical, and it is more than merely speculative". Again, the test is objective.

E. Responsibility for Notification

In terms of responsibility for making the decision as to whether to notify individuals of breaches of their personal information, the proposed PIPEDA model requires that an organization makes the determination independently and then notifies the individual of any breach. This is notably different from the model under the Alberta PIPA, where it is the Alberta Commissioner who may require that an organization to notify the individual of any breach.

F. Offences

Under the proposed PIPEDA model, the breach notification provisions do not create a new offence. This is different from the Alberta model, whereby under the Alberta PIPA, a failure to provide notice to the Alberta Commissioner – i.e. a failure by an organization to "make the right decision" based on the reasonable person test – creates an offence. This distinction is arguably appropriate given the structure of the Alberta PIPA whereby effectively a breach of any obligation under the act (i.e. a breach of compliance, consent, collection, use and disclosure obligations) can result in an offence.

III. Privacy Breach Notification Scenarios Generally

Organizations and their counsel subject to PIPEDA and the Alberta PIPA will obviously need to understand the implications of these rules. Moreover, it is likely that as a result of the instruction of breach notification rules at the federal level and in Alberta, the other substantially similar jurisdictions will follow course and introduce their own respective breach notification rules. In order to assist in understanding how these rules will apply in practice, we have set out below three scenarios designed to illustrate some of the issues organizations and their counsel will need to consider.

Scenario 1: Personal Information in a Stolen Car

A bank branch office in Toronto, Ontario (the "**Bank**"), loses two sets of confidential employee files. There are duplicate copies available for the first set, which are in the form of hard copy files, so the Bank knows the name of the employees in question (the "**Known Employee Files**"). The second set, located on a laptop, was of certain new and transferred employees and had not yet been copied, so the Bank does not know which specific individuals were identified in those files (the "**Unknown Employee Files**").

The files were in the car of an employee of the Bank responsible for human resources matters which was stolen while the employer was at the grocery store. The employee's recollection is that the hard copy files of the Known Employees were under the driver's seat, and that the laptop with the Unknown Employees Files was in the trunk. The files were not encrypted, but access to the laptop was password protected, albeit with a very simple, 6-digit password, which happens to be the same as the customized licence plate on the stolen car. The police believe that it is possible that a person with minimal IT experience could circumvent the password protection and thus access the files on the laptop.

The Known Employee Files contain relatively generic and non-sensitive information about the employees' work records. However, one of the employee files references the fact that the subject employee, who is a practicing Muslim, has requested and been granted access to a storage room for the purposes of periodic prayer throughout the day. At the request of the employee, both the request and the granting of such request, have been kept confidential. The Bank knows that this particular employee, for various

reasons, would like to continue to keep such information confidential. Additionally, the Unknown Employee Files may or may not contain sensitive information.

The stolen car was eventually recovered, two days later. There are no suspects, but the police suspect university student joyriders. The hard copy files of the Known Employee were still under the driver's seat. The laptop with the "Not yet Known Employees" files was still in the trunk, but suffered damage such that it is no longer working. It is not clear that the thieves accessed or tried to access either set of files.

The Bank is a federal work, undertaking or business and is therefore subject to PIPEDA.

Issue 1: Material Breach/ Significant Harm Analysis

The first issue raised by this scenario is that the Bank does not know what information was in the Unknown Employee Files. The Bank has an obligation under the PIPEDA breach notification model to engage in a material breach/significant harm analysis. However, in not knowing what information was contained in the Unknown Employee Files, it is unclear how the Bank would be able to undertake this analysis for the purpose of determining if the incidents are reportable and/or notifiable. This first issue therefore illustrates how conducting the analysis required to assess if a reporting and/or notification threshold has been met will require a certain de minimis amount of information to be available.

Issue 2: Contents of the Notice

Notwithstanding the issue of how the Bank could conduct the required material breach/significant harm analysis for the purpose of determining if notification was required under PIPEDA, the second issue raised by this scenario is how to determine what should be the contents of the required notice PIPEDA would require that the notification contain sufficient information to allow the affected individuals to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it, or to mitigate that harm. Yet if the contents of the Unknown Employee Files are not known to the Bank it will be difficult, if not impossible for the Bank to provide the required information to the affected individuals.

Issue 3: Reporting Threshold (PIPEDA)

The third issue raised by this scenario is whether the breach regarding the Known Employee Files passes the material breach threshold such that it is reportable under PIPEDA. In order to determine this, the Bank would need to establish whether the breach passes the "real risk of significant harm" threshold such that they are notifiable under PIPEDA.

PIPEDA defines "significant harm" as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of

property. Again, PIPEDA appears to effectively deem all of the above kinds of harm as being "significant", while in fact "damage to relationships", "loss of business or professional opportunities" and "damage to or loss of property", for example, may not be significant, depending on the degree. Moreover, the test is an objective one.

There are some nuances, however, to the application of this test in practice. For example, in the case of the Muslim employees, while (a) subjectively, it is known that the employee in question would consider the information regarding his request for religious accommodation to be very sensitive and confidential, (b) *objectively*, it is not clear that a reasonable person would consider that the fact that an employee wishes to arrange for a space for prayer would cause "humiliation", "damage to reputation or relationships" or "loss of business or professional opportunities".

Additionally, it is unclear how, objectively, this scenario is to be assessed. For example, under this objective test, is it proper to assume that there is a certain level of Islamophobia in the general public, which should be a factor considered in reviewing this situation objectively? Unless it was a Bank employee who stole the car, it is unlikely that this information regarding religious accommodation become available to another Bank employee. Arguably, that fact pattern diminishes the likelihood of humiliation, etc. even more.

If this is a subjective test, however, should the specific circumstances of this one employee even be properly considered? The next issue set out below explores this question further.

Issue 4: Reporting Threshold (Alberta PIPA).

As discussed above, the reporting thresholds under PIPEDA and the Alberta PIPA are different. While this fact pattern is set in Ontario, what would be the result if the same breach happened to an organization governed by the Alberta PIPA? As such, the fourth issued raised by this scenario is whether the breach regarding the Known Employee Files passes the "real risk of significant harm test " so that the breach would be reportable and notifiable under the Alberta PIPA.

Alberta Information Sheet 11, like the proposed PIPEDA model, lists "humiliation or damage to one's professional or personal information." Again, objectively, it is not clear that the information regarding this religious accommodation would meet those two criteria. Alberta Information Sheet 11 also states, however, that: "The test is an objective one: whether a reasonable person would consider the harm to be significant. In other words, *an organization does not have to consider whether a particular individual* would consider the harm to be significant, only whether the ordinary person would consider the harm to be significant." (emphasis added). In this case, then, under the Alberta PIPA, it is unclear whether the organization suffering the breach should even consider the specific concerns of the employee regarding potential sensitivity.

Issue 5: The Impact of Facts on Determining the Real Risk of Significant Harm

The fifth issue raised by this scenario is how the facts relating to the recovery of the stolen car affect the analysis as to whether there is a "real risk of significant harm". The proposed PIPEDA model describes the determination of a "real risk of significant harm" as including a review of the following relevant factors: sensitivity of the personal information; and probability (i.e. risk) of misuse. In other words, as noted above, sensitivity of info + probability = harm, with there then being required an evaluation as to whether the harm is significant. In this context then, does the recovery of the stolen car affect the probability factor, and to what extent?

In contrast, Alberta Information Bulletin 11 notes that: "An example of a security breach that would not pose a real risk of significant harm is where the information is recovered before it could possibly be accessed…". In this case, two days is an abbreviated time frame, but the files could possibly have been accessed. However, if the thieves were focused on joyriding in the car, as is suspected, it may not be likely that they found the laptop, or if they did, if they even endeavoured to try and open it. Similarly, it is not clear that the joyriders found the files under the seat.

Moreover, Alberta Information Bulletin 11 also notes that a breach may not pose a real risk of significant harm "…where the information is protected (e.g. encrypted) such that the information could not reasonably be accessed by an unauthorized individual.". Here, therefore, there is a question as to what skills are attributed to the thieves – should they be considered to be lay persons, technologically speaking, or someone with basic (or even advanced) IT skills? Such assumptions could radically change one's perception of the risk of significant harm. So too would these assumptions change the analysis based on facts such as the information not being encrypted, but password protected. Additionally, if the standard of password protection does not meet industry standards, should that be part of the analysis of real risk of significant harm?

Scenario 2: Website/Network Security Breaches

As the result of implementing a new series of software applications at a small e-commerce company, the CTO discovers that one employee has access through their desktop computer to all 5000 of the company's customers' credit card information . This employee has no "need to know" this information for his job function. When confronted, the employee professes to not knowing that he had such access, never mind having actually ever accessed this information. The recently completed implementation means that it is not possible to assess whether access was ever made using the computer. Even if such access could be determined, the company is designed with an open-concept floor plan, such that anyone could have accessed the customer information.

The same e-commerce company, several months later, realizes that, due to human error, for the past two months the unsecured beta version of its new e-

commerce website has been operating in production, such that the company has therefore been collecting customer credit card information through an unsecured site. While there is no evidence of any breach in the security of the database in either of the two months, there is evidence that at one point in the second month the network was accessed by an unauthorized person.

As a result of investigating the breach of network security, it is determined that the person making such unauthorized access was an ex-employee of the company.

The company is in Ontario, such that PIPEDA applies.

Issue 1: Reporting Threshold

In this scenario, the company would need to consider whether the breach regarding this customer information passes the material breach threshold such that it is reportable under PIPEDA. Relevant factors would include the fact that financial information (i.e. credit card) information may have been at risk, and that more than one individual may have affected by the breach.

Issue 2: Systemic Problems

The PIPEDA threshold for reporting to the Federal Commissioner is an objective test that requires a "material breach of security safeguards", where relevant factors to consider include sensitivity; number of individuals; and a subjective assessment of company as to whether the breach is reflective of a systemic problem. In light of this latter factor, the Company will need to consider whether the existence of two potential breaches at the same company is (a) indicative of a systemic problem, or (b) too different for that to be the case. The former argument is assisted by the fact that (i) both breaches are in respect of the same type of information – credit card information; (ii) both potential breaches were due to failures to adequately ensure IT-related safeguards, and (iii) that one potential breach was related to an existing employee, and the other was related to a past-employee, suggesting a systemic issue with HR/management practices. On the other hand, the company may want to take into consideration that (i) the IT systems involved were different, (ii) the policies involved were arguably different (i.e. policies re existing vs past employees), (iii) the level of control the company had in each case was arguably different (again, existing vs past employees), and (iv) there is no evidence of any actual privacy breach in both cases.

Issue 3: Notification Threshold Real Risk of Significant Harm

The second issue is whether the breach regarding the Known Employee Files passes the "real risk of significant harm" threshold such that it is notifiable under PIPEDA. Recall that under PIPEDA, sensitivity of info + probability = harm. Given this calculus, it is unclear if the real risk of significant harm threshold will be met; more specifically, while the information is sensitive given its financial nature, the actual probability that there was harm is unclear. This uncertainty is the result of it being purely speculative whether there was (a) any

access to the unsecured information sent through the company's website, or (b) any malicious intent, notwithstanding that information may have been generally available in the company's office. In other words, it is important to consider at what point, if any, the fact that there could have been harm should equate to an assumption that there was in fact harm.

Issue 4: Evidence Required for Notification

The third issue raised by this scenario is whether the fact that the opportunity for unauthorized collection of personal information existed for a prolonged period of time means that such collection should deemed to have taken place, even without any evidence to support such conclusion. Similarly, consider whether other factors such as the breach in the network (albeit not in the database) should have on the analysis. One might argue that the longer the possibility of unauthorised collection exists, and the more factors that exist that could lead to unauthorised collection, the more willing one should be to assume there has been unauthorised disclosure, such that notification may be required under PIPEDA.

Scenario 3: National Breach

A national luxury retail company, with stores across the country, suffers a loss of customer information at one office in Ontario. The information in question is the customer's contact information, and the fact that they are "VIP" customers. While this status is conferred on those customers than spend more than a certain amount annually at the company's stores, that specific monetary threshold is policy-driven and was not set out in the lost customer information.

An individual informally determines that this breach has happened, and complains to the Federal Commissioner. The Federal Commissioner wants to determine if the company should have reported the breach to her office pursuant to Section 10.1(1), as being a "material breach of security safeguards". Only a few of the individuals in the customer information were identified as VIPs, however, based on the facts of the loss the Federal Commissioner suspects that other offices in other provinces may have suffered a similar breach. To her knowledge, there has not yet been a relevant complaint made against the company in any of the other provinces. She would like to raise the issue with the privacy commissioners in other Canadian jurisdictions, in order to assess the scope of the potential breach.

The company determined that, based on the facts of the disclosure, (a) it was not necessary to notify the VIP individuals of the privacy breach, on the basis that it was not reasonable in the circumstances to believe that the breach created a real risk of significant harm to the individual, and (b) there was no "potential breach of security safeguards", after taking into account, among other factors, the number of individuals involved, such that reporting to the Federal Privacy Commissioner was not required. In the context on either issue, the Federal Commissioner is not convinced that the company has made the correct decision. The company is

governed by PIPEDA, as well as other provincial privacy legislation.

Issue 1: Whether Personal Information is Sensitive

The first key issue to consider is whether the personal information in question – the VIP status of customers – should be considered to be sensitive. Certainly, the VIP status is based on the income of individuals. Therefore, knowing that an individual was a VIP would given, at least to employees of the company, the knowledge that these individuals were in a certain income bracket. However, the information of its own would not provide any information to a third party unfamiliar with the company's operations given that actual income was not listed on the VIP status list.

Issue 2: Breadth of Breaches

This scenario also raises the issue as to whether the possibility of related breaches in other jurisdictions might be relevant to the determination, in any one jurisdiction, as to whether a breach is material.

Issue 3: Communication by Privacy Commissioners

To what extent can a privacy commissioner liaise with his or her colleagues in other jurisdictions to assess whether a breach is material? PIPEDA imposes an obligation of confidentiality on the Federal Privacy Commissioner in respect of "any information that comes to [its] knowledge as a result of performance or exercise of any of [its] duties or power" in respect of protection of personal information in the private sector.[17] Query therefore whether this falls either within (a) the Section 20(3) exemption that lessens these constraints where it is it necessary to conduct an investigation or audit, or establish the grounds for findings and recommendations, or (b) the Section 20(2) exemption, which allows the Federal Commissioner to make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so.

Note that Alberta has a confidentiality restriction, and an exemption under its breach notification regime which is identical to Section 20(3) of PIPEDA. However, consider whether disclosure by the Alberta Commissioner, if any, in response to the disclosure by the Federal Commissioner, falls under the same exemption. This point is debatable given that such a disclosure by the Alberta Commissioner might not be considered to be part of Alberta conducting its own investigation.

Finally, one should consider whether the Federal Commissioner could use Section 20(2) of 20(2) to itself notify the affected individual, where the Federal Commissioner is not convinced that the company has made the correct decision in respect of breach notification. While individuals so affected by breaches might support such disclosures by the Federal Commissioner, such a disclosure might arguably be contrary the intent of the proposed PIPEDA amendments (in contrast to the model under the Alberta

PIPA) which, in effect, grant each organization the discretion to determine when disclosure is required.

IV. Conclusion

The introduction of a breach notification and reporting regime is an important development in Canadian privacy law. While it will take some time to fully appreciate how the Canadian privacy breach regime will operate in practice, it is important for counsel and organizations subject to this regime to consider its implications in advance so that, in the case of an occurrence of a privacy breach, they will be prepared to quickly address the issues within the required time frames.

---

[1] While certain Canadian privacy law is the result of the common law, its effect is limited and outside the scope of this paper.

[2] At the sub-federal level in Canada, there are both provinces and territories. For ease of reference, use of "provincial" and similar terms in this chapter refer to both Canadian provinces and territories.

[3] Accordingly, references to the Canadian privacy law regime in this paper are, unless otherwise noted, references to the Canadian private sector privacy law regime.

[4] S.C., 2000, c. 5. In particular, Part 1 of same. Other parts of PIPEDA seek to clarify evidentiary and functional equivalence issues regarding e-documents and e-signatures.

[5] Applying, per PIPEDA s. 4(1)(b), "to every organization in respect of personal information that…is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business"

[6] More specifically, where a province has enacted "substantially similar legislation" to that of PIPEDA, the Governor in Council may by order exempt organizations or activities subject to such provincial legislation from the application of Part 1 in respect of the collection, use or disclosure of personal information that occurs within that province

[7] An Act respecting the protection of personal information in the private sector, S.Q., 1993, c. 17.

[8] Personal Information Protection Act, S.B.C. 2003, c. 63.

[9] Personal Information Protection Act, S.A. 2003, c. P-6.5.

[10] See (a) Lawson v. Accusearch Inc., [2007] 4 F.C.R. 314., (b) PIPEDA Case Summary #2009-09, and (c) the Federal Commissioner's Report of Findings Complaint under PIPEDA against Accusearch Inc., doing business as Abika.com.

[11] PIPEDA, s. 2(1).

[12] As well as the equivalent legislation in British Columbia.

[13] Alberta PIPA, ss. 1(1) and 4(3).

[14] As this paper was being written in January 2011, while Bill C-28 has received Royal Assent, the more substantial PIPEDA-amending bill, had only received first reading in the House of Commons, and, as such, has to make further progress through the federal legislative system before becoming law. Additionally, were a Parliament to be prorogued or an election called – both possibilities given Canada's current minority government status – this legislation would "die" and have to be reintroduced. Regardless, this legislation is important to understand as it would represent the first material revision of PIPEDA since its entry into force.

[15] It may be that the omission of "reasonable person" is linked to the fact that, unlike under PIPEDA, under the Alberta PIPA it is the Alberta Privacy Commission, rather than the organization itself, who makes the decision as to whether to notify.

[16] Notification of a Security Breach – Personal Information Protection Act Information Sheet 11. Available online at http://pipa.alberta.ca/resources/pdf/InfoSheet11.pdf.
[17] PIPEDA, s.20(1).

Caution: What You Post Can Hurt You!

By Robert A. Baugh

THE EXISTENCE of a "generation gap" reveals itself in new ways for each generation. For those of us who witnessed the emergence of rock and roll and long hair, we saw our parents' heads shaking and looks that were either disapproving or simply quizzical.

Today, those same looks are coming from the members of the generation that said not to trust anyone over the age of 30. However, this time, it's not the music or the clothes that demonstrate that "older" people view the world differently than young adults.

The emergence of the use of social media, such as Facebook and MySpace, reveals sharp differences in what the "older" generation views as acceptable conduct and what is seen by the "younger" generation as common communication and expression. When looking at posts or pictures commonly found on young people's social media sites, older folks are thinking: "Why in the world would someone put that out there for the world to see?"

For members of the "older" generation, there has always been a willingness to talk, tell stories, or tell jokes. Sometimes those conversations were appropriate. But, human nature being what it is, sometimes those conversations may have included gossip, coarse language or been politically incorrect. The speaker made judgments about what could be said, based upon the speaker's knowledge of the listener and whether that person was a trusted friend who could hold the conversation in confidence. Of course, that confidence was sometimes misplaced and an inappropriate conversation might be repeated to a third party. But generally, there was a short life cycle to the story and a limit to how many times the story may be repeated. Thus, the speaker took a calculated risk as to whether a confidential story might be repeated or revealed to the wrong person.

Robert A. Baugh is a shareholder with the firm of Sirote and Permutt in Birmingham, Alabama. Robert has a wide-ranging litigation practice that includes business disputes, insurance coverage and bad faith actions and intellectual property and products liability cases also.

Today, those oral conversations continue to take place. However, there is something much more going on. Social media sites have proliferated in popularity among young people. Facebook and MySpace have become omnipresent among high school and college students. The familiarity with instant communications on these sites has led to a huge volume of written material that documents people's communications and thoughts. What's more, photographs of the users, often in compromising situations, are routinely posted.

While many of these writings and photographs on social media sites may be harmless, there is a fundamental difference between these new communications and old-fashioned conversations: There is a long-term record of communications on social media sites. Social media users seem to

lack an appreciation for the permanency of these writings on the Web. So, what was once an off-the-cuff, smart aleck oral response to a friend is now is available for the world to see, even long after the post is written.

I. Social Media Comes to the Attention of Employers

With all of the information that is now so easily accessible, it is not surprising that employers are inevitably viewing these postings. Employers routinely examine social media sites of prospective employees. Additionally, some employers may review social media sites of current employees. Thus, since many of the people that hold executive or supervisory positions in companies are in the "older" generation, the differing views of what is "appropriate" information or photographs to place on the Web can lead to adverse employment decisions for workers who post their thoughts on social media sites.

A recent example of such different viewpoints was demonstrated when the City of Bozeman, Montana adopted a policy requiring job applicants to provide the City with the user's name and log-in information for social media sites. The policy was revoked after an uproar occurred when the policy was publicized in an on-line version of the ABA Journal. [1] This incident confirms that there are two different views of information on social media sites: Employers want to use this information as part of routine screening of job applicants while social media users think such information is "off limits" for prospective employers.

II. Are Posts on Social Media Sites "Private"?

Some social media users may believe that their privacy is being invaded by third parties who go to their site. However, postings on social media sites are generally not treated as "private." This may come as a surprise to someone who uses privacy settings on their site so that the public does not have access to all of the writer's communications.

While there are innumerable ways for these issues to arise, the most common situation may be where a plaintiff brings suit for personal injuries. Social media sites, where a plaintiff may be inclined to post pictures and comments about his personal life, are natural fodder for an enterprising defense lawyer. Courts have generally been unsympathetic to parties who have alleged that postings on social media sites should be considered "private." Even where the party used a privacy setting on the site, the courts are unlikely to keep such information confidential.

The rationale behind these legal decisions is two-fold: (1) There can be no expectation of privacy in postings on social media sites and (2) The defendant should be able to discover statements from a plaintiff that potentially contradict the plaintiff's testimony about the extent of the plaintiff's injuries. [2]

Requests for discovery of the plaintiff's social media site, including those areas ostensibly labeled as "private", have resulted in several courts issuing orders allowing such discovery. In one case, the Court noted that the Facebook policy states that "it helps you share information with your friends and

people around you," and that "Facebook is about sharing information with others."[3] The New York judge allowed the defendant to obtain access to the plaintiff's social media sites, including sections marked "private" or that had been deleted. The Court also noted the following from a similar Canadian decision:

> To permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.[4]

Courts have also noted that when creating the Facebook and MySpace accounts, the plaintiff consented to the fact that personal information would be shared with others, notwithstanding the privacy settings. Indeed, that is the very nature and purpose of these social networking sites. Since the plaintiff knew that this information may become publicly available, claims that the plaintiff had a reasonable expectation of privacy in these postings rings hollow.[5]

These cases reveal the inherent conflict between the court system and social media users. An important goal of discovery is to allow counsel to determine whether the opposing party is being truthful in the claims that are asserted. The tools that litigators use in discovery allow lawyers to cast a wide net to gather factual evidence. As a result, even where a plaintiff has ostensibly taken steps to keep information on a social media site "private", the rules of discovery will likely trump these self-set privacy labels.

III. Social Media in the Workplace

Many employees acknowledge that they access social media sites for their personal benefit, while they are at work.[6] Additionally, the fastest growing segment of new users of social media are people over the age of 55. Thus, it is reasonable to predict that increasing numbers of employees will be accessing social media while at work.

Employers may have concerns about the time that employees are spending on social media sites during work hours and the accompanying loss of productivity. But, there can be more serious issues that arise where the actions of the employees directly impact the employer.

One well-known example of a YouTube prank gone bad involved Domino's Pizza. Several employees filmed a fictitious incident in the kitchen of a Domino's restaurant. The video purported to show many gross activities of employees, which were obvious health code violations, if they had been true. Within days, the YouTube video had been seen by more than a million viewers and was reported on national television.[7]

In addition to embarrassment or harm to a company's brand, employees' postings can result in legal entanglements. In *Pietrylo v Hillstone Restaurant Group*,[8] employees of a New Jersey restaurant created a MySpace group where they "privately" posted derogatory and graphic sexual statements regarding the restaurant's management,

patrons and policies. After a manager obtained access to the password-protected site, two employees were terminated for their comments posted on the site.

A New Jersey jury found that the employer violated the Federal Stored Communications Act by secretly monitoring the employees' postings on the private password-protected Internet chat room. There was evidence that the employee who gave the manager access to the site may have done so under duress. While the Court found that no free speech issues were implicated because the blog did not implicate matters of public concern, the jury verdict was upheld. This case illustrates the need for employers to strike an appropriate balance between monitoring employees' on-line postings and invading the employees' privacy.

A. Public Employers

In *City of Ontario v Quon*,[9] the U.S. Supreme Court unanimously held that a public employer's review of an employee's text messages on a device issued by the employer was a reasonable search under the Fourth Amendment. Here, a pager was issued to the employee by the City. The City maintained a computer policy which made clear that employees should not have any expectation of privacy in communications when using the City's equipment. The City's employees were later made aware that this policy would apply to pagers.

When the employee exceeded the allocated number of text messages per month, the City reviewed the messages and found that the excessive text messages made during work hours included many messages of a personal nature. When disciplined for violating the City's policy, the employee objected and claimed that his privacy had been invaded.

The Supreme Court found that the employer had a right to see text messages sent and received on the employer's pager. The Court concluded that, even assuming an expectation of privacy in the text messages, the search performed by the City was reasonable under the circumstances. As a result, the search was not in violation of the Fourth Amendment. This decision confirms the importance for an employer to implement a clear policy that addresses privacy expectations in communications by employees on employer-issued equipment.[10]

The Eleventh Circuit recently addressed a claim of gender discrimination where a female firefighter posted photographs in the private section of her MySpace page.[11] These photographs showed the plaintiff with other members of the fire department, as well as personal photographs that revealed her in various states of undress. She brought a claim of gender discrimination after she was terminated for posting unauthorized photographs on her MySpace page. However, her discrimination claim was rejected when she could not show that other employees had been treated differently than her.

Finally, the United States Supreme Court has upheld a City's right to terminate a police officer where his off-duty conduct brought disrepute to the department and was contrary to the goals of professionalism of the police force.[12] While not involving social media, this

same rationale will likely permit an employer to discipline an employee based on unprofessional off-duty conduct involving social media. This is especially true where there is a nexus between the off-duty conduct and the workplace.

B. Private Employers

An increasingly common practice is for employers to closely monitor activities of employees while on the job. GPS units can track an employee's vehicle; software programs can monitor keystrokes at an employee's computer; telephone calls may be recorded; e-mail messages may be reviewed; and surveillance of work areas is now commonplace. While one may question whether George Orwell's world of 1984 has become reality, today's place of employment clearly affords little privacy to an employee.

While such monitoring at the workplace is commonplace, the proliferation of social media sites, such as Facebook and MySpace provides new opportunities for employers to be made aware of activities of employees while they are away from the office. For example, if an employee "friends" a co-worker or supervisor, those people are granted access to a great deal of information about what the employee is doing in his or her spare time.

What is the employer permitted to do when the employee is found to be engaging in inappropriate or illegal activity while away from the office? Is it permissible to discipline or terminate an employee for such actions?

What about an employee "blog" that raises political or social issues? What if the employee's view point is contrary to the position of the employer? If so, what causes of action may be available to the employee who receives this discipline? Isn't the employee being treated unfairly based on his/her right to free speech? Is the employee's privacy being invaded?

As a general rule, claims based upon free speech and the First Amendment are applicable only against State actors.[13] So, private employers should not be subject to such claims. However, private employers may find themselves accused of violating state laws that provide additional protections to employees while away from the job.

IV. Statutes That May Affect Social Media

A. State Privacy Laws May Impact Social Media

In recent years, several states have enacted laws that prohibit employers from interfering with lawful conduct of employees while off-duty. [14] Many of these laws were intended to protect workers who smoked from discrimination. However, these laws have also been used to challenge actions by employers who attempt to monitor off-duty activity, such as dating, by employees.

For example, New York's privacy law prohibits discrimination against an employee who participates in "legal recreational activities outside work hours." [15] The statute defines "recreational activities" as "any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for

recreational purposes, including but not limited to sports, games, hobbies, exercise, reading and the viewing of television, movies and similar material."[16]

To date, there have not been any reported decisions that address the question of whether the use of social media or blogging can be considered "recreational activity." But, there is no obvious reason why such activities, while done on personal time, should not fall within the protection of these statutes. As a result, in states with such privacy laws, employers will likely be constrained from taking disciplinary action against an employee for blogging or social media activity, so long as the employee does not disparage the employer or disclose trade secrets.[17]

B. Does the National Labor Relations Act Protect Comments About an Employer on a Social Media site?

In November 2010, the National Labor Relations Board ("NLRB") filed a complaint against American Medical Response of Connecticut (AMR). This is the first case where the NLRB has taken the position that workers' criticisms of their boss or employer are generally protected activity and that employers may not punish workers for such statements.

This complaint arose after an employee posted negative comments about her supervisor on her Facebook page. The postings were made on the employee's home computer and on her own time. Several co-workers joined in and offered supporting comments of their own about this supervisor. One month later, the employee was fired.

The employer contends that the postings violate policies of AMR which prohibit:

> Posting of "disparaging, discriminatory, or defamatory comments when discussing (AMR) or the employee's supervisors, co-workers, and/or competitors on the Internet;
>
> "(r)ude or discourteous behavior to a client or co-worker; and
>
> the use of language or action that is inappropriate in the workplace whether racial, sexual or of a general offensive nature."

The NLRB conducted an investigation and concluded that the postings by the employee constituted protected activities under the National Labor Relations Act (NLRA). Generally, Section 7 of the NLRA protects the rights of workers, in both union and non-union settings, to communicate with each other about wages, hours, and other terms and conditions of employment. Thus, the NLRA restricts employers from interfering with employees' attempts to "improve their lot as employees through channels outside the immediate employee-employer relationship."[18] Additionally, an employer's general policies can violate the NLRA if they "reasonably tend to chill employees in the exercise of their Section 7 rights."[19] Such a policy can be deemed an unfair

labor practice by an employer for simply maintaining such a policy.

The NLRA prohibits employers from punishing workers, whether union or non-union, for discussing working conditions or unionization. The NLRB's position is that AMR's social media policy is "overly broad" and improperly limits employee's' rights to discuss working conditions among themselves.

The NLRB contends that the termination of the employee unlawfully interfered with those protected activities and discouraged others from engaging in those same activities. Thus, the NLRB is seemingly doing away with any distinction between airing criticisms and concerns at the water cooler and posting these same concerns on the Web.

This issue may not be big a problem for employers in right to work states. There, an employee can be terminated for any reason, so long as it is not an illegal reason. But in other states, postings that arguably disparage a co-worker, supervisor or employer may prove to be fertile ground for employees and their lawyers who contend that discipline is based upon private communications posted on social media sites.

V. Application

A. Inappropriate Conduct Involving Social Media Can Lead to Discipline

As a general rule, employers should not take disciplinary action against an employee for lawful off-duty conduct unless the conduct falls into one of the following categories:

1. A conflict of interest is created, such as performing work for a competing company;
2. The employee's job performance is impaired. This can occur with late-night second jobs that prevent the employee from obtaining sufficient rest to perform as required; or
3. Where the conduct compromises the employee's judgment. A common example is where a supervisor dates a subordinate and the supervisor must continue to evaluate the job performance of the subordinate.

Conflicts of interest issues can arise by employees' use of social media or blogging. For example, blogs written by employees can create concerns for an employer. A blog is the author's observations about life in general, or more specific issues which can involve politics or other social issues.[20] However, a blog also allows others to post statements or opinions to the site. Thus, a blog can create a forum for ideas that can be read on a world-wide basis. These statements by bloggers, or others on the site, can be attributed to the employer. So, the employee should conspicuously state that the views expressed on the site are personal to the employee.

Employers are justifiably concerned about the loss of copyrights or trade secrets by the posting of blogs by employees. But, traditional company policies concerning the protection of company information should apply to the blogosphere. Employers need to be clear

that intellectual property protections apply to these blogs.

Some companies now sponsor blogs and encourage employees to contribute to these blogs. Given the fast-paced nature of the writings on these blogs, companies may be concerned about the content that is posted therein. Again, company policies against discrimination, harassment and defamatory statements should apply to prevent such statements that may be made in company-sponsored blogs.[21]

B. Social Media Policies

The action by the NLRB in the AMR case demonstrates that an employer who maintains an overly broad social media policy may face a challenge that the policy constitutes an unfair labor practice. Such a charge may be brought even where the policy has not been used to pursue enforcement of the policy against an employee.

Employers should review their social media policies to determine if they are susceptible to an employee's claim that that the policy will "reasonably tend to chill employees" in the exercise of their rights to discuss wages, working conditions and unionization.

The first decision to be made by an employer is whether the policy will apply only to postings made at work or whether the policy will also address off-duty communications. As discussed previously, there are laws in several states that prohibit an employer from terminating an employee for lawful off-duty conduct. Therefore, an employer, especially in those states, should avoid blanket pronouncements that inappropriate statements, even made off-duty, will be grounds for discipline or termination.

It should be noted that these laws only protect off-duty activities that are otherwise legal. So, if an employee is blogging and making statements that are defamatory or may lead to a hostile work environment, the employer should not be prohibited from taking action against the employee for such statements.

C. Suggestions for Employers

While the drafting of a social media policy for employers is beyond the scope of this article, the following topics should be addressed by employers when drafting such a policy:

- If an employee writes about his or her employer, the employee must use his or her real name and make clear that any opinions offered are his/her own and do not represent the company's positions, strategies or opinions.
- If an employee writes positively about the Company's products or services, the employee must disclose the employee's relationship with the Company.[22]
- The privacy rights of others must be respected in posts and comments.
- Posts are not permitted that may be considered obscene, threatening, defamatory, harassing or embarrassing to others.
- Employers should clearly address the level of privacy that

employees expect in their work computer systems, including e-mail and use of the Internet. Courts will consider whether an employer has an electronic communications policy when determining whether an employee had a reasonable expectation of privacy in the use of the company's computer system. With such a policy in place, an employer will have more freedom to take disciplinary action against an employee who misuses the company's computer system.

- Even for off-duty posts, the policy should clearly state that the employer will monitor the employee's use of social media and that the employee should not have an expectation of privacy in any post or blog.
- Employees must comply with all other company policies with respect to electronic communications. For example, statements that can be considered discriminatory or harassing are prohibited.
- The company's computer system cannot be used to download or distribute pirated software.
- No electronic communication about internal company matters.
- Confidential or proprietary information that may rise to the level of company trade secrets may not be disclosed.
- Ban references to customers or clients. The Company's relationships with customers or clients are valuable company assets. As such, the identity of these relationships should not be publicized without express permission.
- Obtain permission to use the company's intellectual property, such as materials protected by trademarks or copyrights.
- Managers should not send "friend" requests to subordinates, even when off-duty.
- All employees should be free to reject a "friend" request from any other employee.
- The policy should include a clear warning that a violation of the social media policy will be grounds for discipline, up to and including termination.

D. Suggestions for Employees

- Do not post inappropriate pictures or images.
- Be careful about any comments concerning your job or supervisors. While complaining about the Boss to a confidant is nothing new, posting these complaints for the world to see is just asking for trouble.
- Assume that everything you write on-line will be forwarded to someone else. This goes back to the question: Would you want this published on the front page of your local paper? If not, you need to re-think what you are writing.
- Fair use and copyright laws apply to your on-line writings. The improper use of logos or

other authors' writings can get you in legal hot water. While on-line posts can seem more informal than a published article, you cannot ignore the intellectual property rights of others.

- Many companies now encourage employees to post information about the company or its products. If you, as an employee, choose to write on the Web, clearly state that the statements and opinions are yours, and not those of your employer. Take care not to reveal confidential or proprietary information about the company, such as company strategy, upcoming product releases or financial information about the company.
- Use common sense. Think twice before you post something that is "pushing the envelope." Once you post a writing that is inappropriate or discloses information that is proprietary to your employer, you may not be able to repair the damage. You are solely responsible for what you write. So, ask a friend or co-worker for a second opinion before you publish your thoughts for the world to see.

VI. Conclusion

The informal nature of social media can mislead users into thinking that posting inappropriate material is "no big deal." However, while the wall between work and personal life continues to be chipped away, there are consequences in the workplace for postings on social media sites.

In the legal world, words matter. Those words have significance, whether written in a formal document or quickly typed at home on a web site when voicing a complaint about a supervisor. For that reason, members of the "younger" generation who are comfortable with social media must recognize that the legal system can impose consequences for what you write. As a result, an employee can face adverse consequences at work for comments that were mistakenly assumed to be personal, private and made on the employee's own time.

---

[1] Molly McDonough, *Town Requires Job Seekers to Reveal Social Media Passwords*, ABA J. LAW NEWS NOW, June 19, 2009, http://www.abajournal.com/news/article/town_requires_job_seekers_to_reveal_social_media_passwords/

[2] Robert S. Kelner & Gail S. Kelner, *Social Networking Sites and Personal Injury Litigation*, N.Y. L.J., Vol. 242, Sept. 22, 2009.

[3] Romano v Steelcase, Inc., 907 N.Y.S.2d 650, 2010 N.Y. Slip. Op. 20388 (2010).

[4] 907 N.Y.S.2d at 655.

[5] Leduc v Roman, 2009 Carswell Ont 843 (Feb. 20, 2009).

[6] SOCIAL NETWORKING AND REPUTATIONAL RISK IN THE WORKPLACE: DELOITTE LLP, 2009 ETHICS AND WORKPLACE SURVEY RESULTS, http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf .

[7] Stephanie Clifford, *A Video Prank at Domino's Damages its Brand*, N.Y. TIMES, April 15, 2009, *at* http://www.nytimes.com/2009/04/16/business/media/16dominos.html?_r=2.

[8] 2008 WL 6085437 (D.N.J. 2008) (order denying in part defendant's motion for summary judgment). *See* Konop v Hawaiian

Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) (secret monitoring of password protected website visited by an employee while at work violated the Federal Stored Communications Act).

[9] 130 S. Ct. 2619 (2010).

[10] Posts that complain about employer and supervisor can be grounds for discipline or termination. *See* Spanierman v Hughes, 576 F. Supp.2d 292 (D. Conn. 2008) (teacher firing for inappropriate MySpace communications with students upheld by District Court); *but see* Garcetti v. Ceballos, 547 U.S. 410 (2006) (public employee statements made pursuant to official duties, even if made while off-duty, not protected by First Amendment).

[11] Marshall v. Mayor of Savannah, 366 Fed. Appx. 91 (11th Cir. 2010)

[12] City of San Diego. v. Roe, 543 U.S. 77 (2004).

[13] *See* Golden Gateway Ctr. v. Golden Gateway Tenants Ass'n, 29 P.3d 797 (Cal. 2001).

[14] Such statutes have been adopted in New York, California, Colorado, Connecticut, Montana and North Dakota.

[15] N.Y. LAB. § 201-d(2)(c).

[16] *Id.*

[17] The New York statute clearly provides that it does not sanction employee activity that "creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest." N.Y. LAB. § 201-d(3)(a). New York courts confirm that employees owe a duty of loyalty to their employer and may not disclose confidential knowledge or trade secrets. *See* Bus. Networks of N.Y., Inc. v. Complete Network Solutions, Inc., 1999 WL 126088 (N.Y. Sup. Ct. Feb. 19, 1999), *aff'd*, 696 N.Y.S.2d 433 (App. Div. 1999).

[18] Eastex, Inc. v. NLRB, 437 U.S. 556, 566 (1978).

[19] Lafayette Park Hotel, 326 N.L.R.B. 824, 825 (1998).

[20] Twitter is a web service that provides "microblogging" capabilities.

[21] *See* Varian Med. Sys., Inc. v Delfino, 6 Cal. Rptr. 3rd 325 (Cal. Ct. App. 6th Dist. 2003) (former employees fined after making thousands of posts which included personal attacks on former co-workers) (depublished 85 P.3d 444 (Cal. 2004); Apple Computer, Inc. v. Doe, 2005 WL 578641 (Cal. Super. Ct. Mar. 11, 2005), *order set aside*, O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72 (Cal. Ct. App.), *as modified*, (June 23, 2006) (Apple obtained Order to disclose names of bloggers who allegedly leaked trade secret information to websites).

[22] *See* The Federal Trade Commission *Guides Concerning the Use of Endorsements and Testimonials in Advertising*, http://www.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf. The guides address endorsements by employees.

"A Sign of the Times: Massachusetts Strengthens Protection Requirements for Consumer Information"

By Edward A. Kendall, Jr. and Robert A. Curley, Jr.

WITH THE RISE of the global economy, new challenges arise for business, government and individuals in protecting the financial and personal information of customers from those who seek to misappropriate it. In order to help consumers fight this battle, the Commonwealth of Massachusetts passed legislation that aims to protect consumer information used in business transactions. Massachusetts General Laws Chapter 93H, which affects all types of businesses, attempts to prevent and limit the impact of security breaches in the Commonwealth of Massachusetts when dealing with the personal information of Massachusetts residents. The legislation and related regulation requires the substantial protection of private data through a written information security program as well as specific protections of computer based personal information.

It appears the Massachusetts General Court passed the act related to the protection of consumers' privacy and data in response to several instances of highly publicized breaches of security which affected many Massachusetts residents. It appears the extensive breach of security concerning personal information that occurred at Massachusetts based TJX Companies and its affiliates was a primary instigator behind the legislation at issue. In late 2006 and early 2007, TJX Companies discovered that a group of hackers had gained access to the central database of TJX Companies and had misappropriated consumers personal information as well as financial information for illegal purposes.[1] Based upon early estimates of the damage inflicted by the hackers in the TJX case, it appeared that over 45 million credit and debit card numbers (in addition to driver's license numbers and Social Security numbers) were stolen from TJX and its related companies.[2] In addition, as described by Mr. Pereira, important to note was "[t]he ease and scale of the

Edward A. Kendall, Jr., Esq. is an Associate at the Boston firm of Curley & Curley, P.C. His practice involves the defense of product liability, personal injury, municipal law and general civil litigation matters. Attorney Kendall is a member of the Defense Research Institute as well as the Massachusetts Defense Lawyers Association.

Robert A. Curley, Jr., Esq. is president of the Boston firm of Curley & Curley, P.C. His practice involves the defense of product liability, catastrophic personal injury cases, general civil litigation and insurance coverage matters. Attorney Curley is a Fellow at the American College of Trial Lawyers. He is a former president of the Massachusetts Defense Lawyers Association as well as a former President of The Foundation of the International Association of Defense Counsel. He is the Director-Elect of the Defense Trial Academy of the International Association of Defense Counsel for 2012.

fraud expose how poorly some companies are protecting their customers' data on wireless networks, which transmit data by radio waves that are readily intercepted."[3] The information contained on those wireless networks would be a major focus of the Massachusetts personal information security measures contained in Massachusetts General Laws. ch. 93H and related legislation as well as regulations.

Massachusetts General Laws ch. 93H relates to the safeguarding of personal information contained in both paper and electronic records. The legislature, in response to the significant data breaches briefly discussed above, provided guidance to the Massachusetts Department of Consumer Affairs and Business Regulation in how to protect important consumer information of residents of the Commonwealth of Massachusetts which is owned or licensed by any person.[4] Mass. Gen. Laws ch. 93H, § 2(a) seeks to "insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer."[5] Importantly, the legislation and accompanying regulation, only require the protection of personal information related to Massachusetts residents.

Mass. Gen. Laws ch. 93H establishes the information to be protected and what individuals, businesses or agencies are required to comply with the section. Mass. Gen. Laws ch. 93H, § 1(a) provides the definition of "data" and "personal information" to be protected. "Data" is defined as "any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics."[6] Such a definition of data is broad and expansive, seeking to capture both electronic and paper records. However, the law requires only that the "personal information" of a resident of the Commonwealth be protected. "Personal Information" is defined as "a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that 'Personal Information' shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."[7]

The legislation only requires the significant protection of "personal information" by a person who owns or licenses such information. A person that simply maintains or stores personal information is subject to a less stringent set of requirements pursuant to Mass. Gen. Laws ch. 93H. Mass. Gen. Laws ch. 93H, §1(a) defines a "person" as "a natural person, corporation, association, partnership or other legal entity."A

"person" does not include a government agency, department, board, or any political subdivision thereof.[8] Once a breach occurs related to personal information, persons that own or license such data are required to report the breach of security to the Massachusetts Attorney General, the director of consumer affairs and business regulation as well as the affected resident.[9] Persons or agencies that do not own or license the data, but maintain or store such personal information are also required to report breaches of security related to such data.[10]

Pursuant to Mass. Gen. Laws ch. 93H as directed by the final legislation, the Massachusetts Department of Consumer Affairs and Business Regulation ("MA Consumer Affairs") issued regulations outlining the standards for the protection of personal information of residents of the Commonwealth of Massachusetts.[11] The regulation, which went into effect on March 1, 2010, "establishes the minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records."[12] It is the objectives as outlined in Mass. Gen. Laws ch. 93H, § 2(a), as described above, which provide the basis for 201 CMR 17.00.

The regulations apply to those who own or license personal information about residents of the Commonwealth, excluding government agencies and/or departments.[13] The regulations require that "[e]very person that owns or licenses personal information about a resident of the Commonwealth…" develop a comprehensive information security program.[14] However, based upon the definition of "owns or licenses" contained in 201 CMR 17.02, it appears the regulation goes beyond the scope of Mass. Gen. Laws ch. 93H to specifically subject those who simply maintain or store such personal information concerning residents of the Commonwealth of Massachusetts to the requirements of the 201 CMR 17.00. A person is considered to own or license such information, pursuant to 201 CMR 17.02, when one "Owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment."[15] Therefore, any person who deals with personal information in a business setting is subject to the requirements of 201 CMR 17.02.[16]

It appears that Massachusetts may be one of the first states in the nation to require a written security information program along with specific computer security requirements from all individuals and/or businesses who deal with personal information of residents of the Commonwealth of Massachusetts. Massachusetts, and specifically the Office of Consumer Affairs & Business Regulation, makes clear that the scope and requirements of the statute as well as the regulation depend upon the scope and size of the business in the Commonwealth. The security breaches and information related thereto will be analyzed on a case by case basis. The statute and regulations highlight the fact that the Commonwealth of Massachusetts will analyze the breaches (and safeguards required of each business) by looking at

the total circumstances of the business at issue.

The Massachusetts General Court (which is the Massachusetts legislature) included the following factors in the final legislation for determining the level of security required of a business: the size and type of the business, resources of the business, the amount of stored data, and the need for security and confidentiality of consumer and employee information.[17] In addition, the safeguards maintained by a person as outlined in Mass. Gen. Laws ch. 93H and 201 CMR 17.00 must also comply with any additional state and federal regulations by which the business may already be regulated.[18]

Persons who own or license personal information were required to be in full compliance with 201 CMR 17.00 by March 1, 2010.[19] The written information security program for a person who owns or licenses personal information has several requirements as discussed in 201 CMR 17.00. 201 CMR 17.00 establishes two sets of requirements in relation to the securing of personal information. The first set, 201 CMR 17.03(2) lists the requirements for the comprehensive security information programs while the second set[20] establishes computer system security requirements to be included in the written, comprehensive security information programs.

I. The Written Information Security Program

The key requirements of 201 CMR 17.03(2) require the person who owns or licenses personal information to maintain a comprehensive information security program. Such program shall include (but not be limited to) the following:

a) Designating one or more employees to maintain the comprehensive information security program.
b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: 1. ongoing employee (including temporary and contract employee) training; 2. employee compliance with policies and procedures; and 3. means for detecting and preventing security system failures.
c) Developing security policies relating to the storage, access and transportation of records containing personal information outside of business premises.
d) Imposing disciplinary measures for violations of the Comprehensive information security program rules.
e) Preventing terminated employees from accessing records containing personal information.
f) Oversee service providers, by:
    1. Taking reasonable steps to select and retain third-party service providers that are

capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and

2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information…

g) Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.

h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrading information safeguards as necessary to limit risks.

i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

II. Computer Security Requirements

The comprehensive information security programs require persons who own or license personal information to provide security systems for technology used by the business. It is in these specific computer security requirements that Massachusetts moves to the forefront in protecting personal information of its residents. Such computer security requirements include secure user authentication protocols, secure access control measures, encryption of transmitted records and files containing personal information that will travel across public networks, reasonable monitoring of systems, encryption of all personal information stored on laptops or other portable devices, for files containing personal information on a system that is connected to the Internet, reasonably up-to-date versions of system security agent software, and education and training employees on the proper use of the computer security system and the importance of personal information security.[21]

Secure user authentication protocols include: Secure access control measures include restricting access to records and files containing personal information as well assigning unique identifications and passwords "that are reasonably designed to maintain the integrity of the security of the access controls."[22]The computer security requirements are required to the extent technically feasible for the person

who owns or licenses the information at issue. Therefore, as with the written information security program, the computer security requirements depend on the size and scope of the business at issue.[23]

III. Notice Requirements of Mass. Gen. Laws ch. 93H

In addition to the stringent security requirements provided in Mass. Gen. Laws ch. 93H and propounded upon in 201 CMR 17.00, the statute requires a person who knows of a security breach regarding personal information they maintain or store to the individuals whose information is involved in the security breach.[24]The person is required to notify the owner or licensor of the information involved, the date of the security breach at issue and steps taken by the person relating to the incident.[25]Persons who own or license personal information have more stringent notice requirements regarding a breach of security related to personal information. Mass. Gen. Laws ch. 93H § 3(b). Persons who own or license personal information are required to notify the attorney general, the director of consumer affairs and business regulation as well as the resident of the breach in security related to personal information.[26]Notice is required once a person or agency knows or has reason to know of a breach of security or when the person or agency knows the personal information was acquired or used by an unauthorized person or for an unauthorized purpose.[27] The person who owns or licenses the information is required to include certain information to the Massachusetts resident upon breach of security pursuant to Mass. Gen. Laws ch. 93H § 3(b).[28] Information to be included is the resident's right to a police report and information regarding security freeze related to the resident's personal information.[29]

The introduction of the stringent security measures represents costly modifications that many businesses, including small businesses, who deal with personal information of Massachusetts residents have to take. It was estimated, in or around October of 2008, that compliance with Mass. Gen. L. c. 93H would cost a business with 10 employees around $9,000 a year.[30] Based upon that estimate, it appears the costs of compliance will be substantial. Furthermore, the Massachusetts Attorney General's Office is allowed to bring a consumer protection action pursuant to Mass. Gen. Laws ch. 93A against a person to remedy violations of Mass. Gen. Laws ch. 93H.

Compliance with the new law regarding personal information security may be costly and cumbersome for businesses large and small, but time will tell whether the personal information of Massachusetts residents will be sufficiently protected by the new legislation. As quickly as the political establishment may be able to establish guidelines and requirements, those who seek to misappropriate the information may be able to establish new means and methods for securing such personal information.

---

[1] *See* Joseph Pereira, *Breaking the Code: How Credit-Card Data Went Out the Wireless Door*, WALL ST. J., May 4, 2007, at A

[2] *Id.*

[3] *Id.*
[4] *See* MASS. GEN. LAWS ch. 93H, §2(a).
[5] MASS. GEN. LAWS ch. 93H, § 2(a).
[6] MASS. GEN. LAWS ch. 93H, § 1(a).
[7] MASS. GEN. LAWS ch. 93H, § 1(a).
[8] *Id.*
[9] *Id* at § 3(b).
[10] *Id* at § 3(a).
[11] 201 CMR 17.00.
[12] 201 CMR 17.01(1).
[13] 201 CMR 17.01(2).
[14] 201 CMR 17.03(1).
[15] 201 CMR 17.02.
[16] *See also* "Frequently Asked Question Regarding 201 CMR 17.00" issued by the Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation dated November 3, 2009.
[17] MASS. GEN. LAWS ch. 93H § 2(a).
[18] 201 CMR 17.03(1).
[19] 201 CMR 17.05.
[20] 201 CMR 17.04.
[21] 201 CMR 17.04 (1) – (8).
[22] 201 CMR 17.04 (2).
[23] 201 CMR 17.04.
[24] MASS. GEN. LAWS ch. 93H § 3(a).
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *See* Ben Worthen, *New Data Privacy Laws Set for Firms,* WALL ST. J., October 16, 2008, B1.

Outsourcing Privacy: Confidentiality Concerns Surrounding Sending Legal Services Overseas

By Amy Sherry Fischer and Lindsey Parke

Amy Sherry Fischer is a shareholder at Foliart, Huff, Ottaway & Bottom in Oklahoma City. She focuses her practice in the areas of products liability, particularly drug and medical products, personal injury, and insurance related matters.

Lindsey Parke was a law clerk at Foliart, Huff, Ottaway and Bottom.

LIKE many other industries that take advantage of lower costs and increased efficiency obtained through outsourcing, the legal industry has begun sending work overseas. The recent economic downturn, as well as increasing costs for legal services and dramatic growth of electronic discovery, has prompted law firms to consider outsourcing as a promising option. In its infancy, legal outsourcing was limited to functions traditionally performed by paralegals and office assistants. Over time, however, many firms have begun outsourcing work that would otherwise be performed by attorneys. Outsourcing legal services raises unique concerns related to privacy.

I. What is Outsourcing?

Outsourcing is the business practice of sending work previously performed inside a company or firm to an outside company for performance.[1] This article focuses on offshore outsourcing, a process through which a portion of a business's activities are relocated and delegated to a third party in a different (offshore) location. The new location ideally allows the business to capture increased efficiency while decreasing labor costs.[2] For example, the time difference between the United States and India, the country to which most legal work is outsourced, can be used to boost efficiency because U.S. law firms can have "a sense of operating on a 24-hour-basis."[3] Corporations are often able to save a tremendous amount of money through outsourcing because the work can be completed at a significantly lower rate than those incurred in the United States.

II. Emerging Trends in Outsourcing

Offshore outsourcing, initially a strategy employed by the business industry, has traditionally consisted of activities such as data processing, call center operation, medical transcription, and software design.[4] Law firms followed suit, and more than three million legal jobs were outsourced offshore in the early years, from 2001 to 2005.[5] Legal outsourcing can consist of sending work to subsidiaries, directly hiring foreign law firms, and delegating work to legal process outsourcers (LPOs).[6] The use of LPOs has increased rapidly as many firms transition from sending only work previously completed by paralegals and legal assistants in the United States to outsourcing more routine legal work.[7] Because corporations have become more cost conscious as a result of the recession, businesses and law firms are looking to cut costs where possible, and legal

budgets in particular have been targeted as a way to reduce costs. As a means to cut costs across the board, many firms have begun to consider greater utilization of LPOs.

India is the main destination for legal outsourcing from the United States. While India's LPO industry is still small, it is growing fast. According to an Indian consulting firm, the number of legal outsourcing companies in India was more than 140 at the beginning of this year, up from just 40 in 2005.[8] India's LPO industry is expected to reach revenues of $440 million by the end of 2010.[9]

India is a particularly attractive outsourcing location to American businesses. American firms are enticed by Indian-educated and licensed attorneys who speak English and can perform legal work at a fraction of the price of their American counterparts.[10] Some experts predict that 80,000 or more legal jobs may be outsourced offshore over the next ten years.[11] As the trend continues toward legal offshore outsourcing, several privacy concerns must be addressed.

III. Privacy Concerns

There are several key ethical considerations in offshore outsourcing of legal services. While outsourcing offers cost-savings, increased efficiency, and convenience, it can also raise questions of security and confidentiality. The United States legal profession places great emphasis on the duty to protect a client's privacy. ABA Model Rule 1.6, for example, addresses the duty of confidentiality and states that a lawyer shall not reveal "information relating to the representation of the client" unless the client gives informed consent or the disclosure is impliedly authorized in order to carry out representation.[12] Additional ethical considerations relating to privacy include protecting privileged communication between the client and attorney as well as preventing unauthorized practice of law through proper supervision.

A. Confidentiality

The duty to protect a client's confidentiality is perhaps the most important privacy consideration related to offshore outsourcing of legal services. Every jurisdiction in the United States protects against disclosure of a client's confidential information. Rule 1.6 charges lawyers with the duty to protect a client's confidences and secrets. Comment 16 to Rule 1.6 explains a lawyer should be vigilant to "act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."[13]

Law firms in the United States constantly remind their employees, both lawyers and non-lawyers, of the crucial importance of protecting a client's confidential information and privacy. Because legal representation invariably includes securing documents containing confidential information, law firm policies generally provide for protection of such documents. Such measures include using code names or numbers to mask identities, restricting access to confidential information to necessary

individuals, and limiting, tracking, and shredding copies.[14] Employees are also instructed on the dangers of accidental disclosure.

While attorneys and law firms in the United States are aware of the duty to protect a client's confidential information, privacy concerns arise with the outsourcing of confidential information to countries where such protections may not be in place or enforced. Firms must first deal with the question of whether a client's confidential information can be transmitted overseas in accordance with U.S. law. Existing local, state, or federal laws may regulate what confidential information can be exported.[15]

Legal questions may also arise in connection with the laws of the vendor country. Some countries, for example, may subject an organization's property to judicial or administrative seizure.[16] A disgruntled employee or creditor of an LPO could seek to seize confidential client information in connection with a suit against the organization. The ease with which private information can be seized depends on the substantive law of the country in which the legal services are being performed.

If a U.S. firm determines that a client's confidential information can legally be transmitted and used overseas, the firm must next ask whether practical safeguards exist to adequately protect a client's confidential information.[17] India's legal system, like that of America, has a common-law basis. Like all foreign jurisdictions in the common- and civil-law traditions,[18] India recognizes that lawyers have a duty to protect client confidentiality. The mere presence of such a duty does not, however, guarantee protections similar to those found in America. Interpretation of a duty like that to protect confidentiality will undoubtedly be influenced by a country's professional culture.[19]

Intimately related to the duty to protect a client's confidentiality is the attorney/client privilege. "Privilege" protects any communication between the client and lawyer for purposes of seeking legal advice. The attorney/client privilege, like the duty of confidentiality, may be construed differently in many countries. Privilege may exist only with outside counsel, as a matter of company policy, or as a contract.[20]

Law firms that seek to outsource overseas must be aware of the dangers of risking clients' privacy by releasing confidential information to those who may not be bound by the same rules of professional conduct. As previously mentioned, different societies espouse different corporate cultures and standards of conduct. Because of this, employees in some cultures may not realize that their norm of discussing work information or high-profile clients may be embarrassing or harmful.[21] ABA Formal Opinion 08-451 warns of the risk that any outside service provider may inadvertently ("or perhaps even advertently") reveal confidential client information to unprivileged or even adverse parties.[22] The risks of bribery, commercial theft, and industrial sabotage or espionage likely vary depending upon the region. Other industries that have experienced intentional mismanagement of private information at the hands of offshore vendors warn against the potential misuse of confidential or private client data.[23]

The outsourcing firm must take affirmative measures to train receiving parties working on a particular client matter on the American application of these rules to avoid inadvertent disclosures of confidences or secrets. Not only do breeches of confidentiality violate the Model Rules of Professional Conduct, they subject American firms to tort liability and disciplinary action. American attorneys have been held liable for both inadvertent and intentional disclosures of confidential information.[24]

B. Unauthorized Practice of Law

Law firms outsourcing overseas should be aware of the potential threat to clients' privacy posed by unauthorized practice of law. Non-lawyers and lawyers not licensed in the United States performing outsourced legal work raise significant ethical questions. The legality of outsourcing of legal services is widely accepted, but several authorities suggest "that supervision of all work by a fully-qualified lawyer is 'key.'"[25]

The ABA Standing Committee on Ethics and Professional Responsibility described outsourcing as a "salutary trend" in the global economy in its Formal Opinion, "Lawyer's Obligations When Outsourcing Legal and Non-legal Support Services" ("ABA Opinion").[26] The ABA Opinion advised that the supervisory requirements of Rules 5.1 and 5.3 apply to attorneys outsourcing legal and non-legal support services.[27] Rule 5.1(b) requires that "[a] lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of the Professional Conduct."[28] Rule 5.3(b) details similar obligations with regard to non-lawyers. It provides that lawyers who retain or associate with non-lawyers must "make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer."[29]

Workers to whom confidential client information is outsourced are often not licensed to practice law in the United States. While those unlicensed workers may not be subject to U.S. ethics rules, the law firms and attorneys employing them certainly are. Outsourcing lawyers must therefore "ensure that tasks are delegated to individuals who are competent to perform them, and then to oversee the execution of the project adequately and appropriately."[30] If LPO employees were to inadvertently compromise confidential client information, for example, the supervising attorney could be held liable. Such a possibility is even more reason to attempt to guarantee protection of client privacy.

To meet the requirements laid out in Rules 5.1 and 5.3, the ABA Opinion suggests that "a lawyer outsourcing services for ultimate provision to a client should consider conducting reference checks and investigating the background of the lawyer or non-lawyer providing the services as well as any non-lawyer intermediary involved, such as a placement agency or service provider."[31] The opinion recommends heightened supervisory practices when privacy and confidentiality concerns are at stake:

> Depending on the sensitivity of the information being provided to the service provider, the lawyer should consider investigating the

> security of the provider's premises, computer network, and perhaps even its recycling and refuse disposal procedures. In some instances, it may be prudent to pay a personal visit to the intermediary's facility, regardless of its location or the difficulty of travel, to get a firsthand sense of its operation and the professionalism of the lawyers and non-lawyers it is procuring.[32]

The ABA Opinion emphasizes that, when it is apparent that significant dissimilarities exist between the professional cultures of the United States and the nation to which work is outsourced, "it will be more important than ever for the outsourcing lawyer to scrutinize the work done by the foreign lawyers – perhaps viewing them as non-lawyers – before relying upon their work in rendering legal services to the client."[33]

Practical application of the ABA Opinion's suggestions seems more difficult and less effective than it would suggest. Some believe the guidance is little more than "steps in hiring *any* vendor for any large project," in the U.S. or abroad.[34] Investigating the security of a provider's premises and its refuse disposal procedures may realistically do little to ensure confidential information is kept secure.

The trend toward outsourcing more complicated legal work, such as e-discovery projects, raises significant concerns about the unauthorized practice of law. It is not difficult to imagine a situation in which non-lawyers working for an LPO accidentally reveal confidential client information to the detriment of both the client and the lawyer, who could be sanctioned for improper supervision.[35] The fact that the U.S. attorney paid a personal visit to the facility may (or may not) help the attorney's defense, but it does little to actually protect the client's privacy.

IV. Recommendations

Law firms in the U.S. are increasingly utilizing offshore outsourcing as a way to cut costs and increase efficiency. This trend is not likely to end soon. Law firms will continue to make use of LPOs in light of downward pressure on costs and increasing utilization of technology. The ABA's eager acceptance of legal outsourcing has removed some unease surrounding the practice, and law firms are proceeding with outsourcing at lightening speed. Despite increasing acceptance and employment of legal outsourcing, ethical concerns regarding client confidentiality and privacy exist. Awareness of privacy concerns will allow outsourcing attorneys to better protect their clients and themselves. Some recommendations to improve the practice of legal outsourcing include disclosing any use of outsourcing and obtaining client consent, contracting for all confidentiality obligations and restrictions with companies receiving confidential information, and limiting access to confidential information.

A. Disclosure and consent

The previously mentioned ABA Opinion addressed the need to provide information to the client concerning the utilization of offshore outsourcing. Prior to the 2008 ABA Opinion, most U.S. lawyers equated disclosure requirements in the case of outsourcing to disclosure requirements in the case of temporary lawyers. In 1988, the ABA Committee on Ethics and Professional Responsibility held that a client was not entitled to full disclosure that a temporary lawyer was performing its legal work.[36] This opinion was based on the assumption that the temporary lawyer in question would be carefully supervised and controlled by a licensed attorney. The 2008 ABA Opinion refuted this assumption in the case of offshore outsourcing. It recognized that such a high degree of supervision essentially making the supervised lawyer tantamount to an employee will typically not exist in the context of offshore outsourcing.[37] The ABA Opinion strongly advocated obtaining client consent in situations where client confidentiality is a concern:

> Thus, where the relationship between the firm and the individuals performing the services is attenuated, as in a typical outsourcing relationship, no information protected by Rule 1.6 [concerning confidentiality] may be revealed without the client's informed consent. The implied authorization [in the Rules] to share confidential information within a firm does not extend to outside entities or to individuals over whom the firm lacks effective supervision and control.[38]

Outsourcing remains a highly controversial practice and many clients do not want their confidential information sent overseas.[39] Privacy concerns may lead a client to choose a firm that utilizes in-house paralegals rather than less costly workers overseas. While some state bars differentiate between lawyers and non-lawyers when deciding whether client consent is necessary for outsourcing, informed consent should always be obtained when there is a possibility that client confidences and secrets will be disclosed. Furthermore, client consent is a necessary requirement of most privacy legislation that allows companies to outsource personal information.[40] For practical purposes, it seems prudent to inform a client of the possibility of legal outsourcing as early as the situation allows. Making the disclosure and gaining consent before steps to outsource are initiated is the safest move for all parties involved.

B. Contract confidentiality obligations and restrictions

Despite the inherent difficulties involved in closely supervising overseas employees, supervisors are obligated to make "reasonable efforts" to ensure employees follow the rules of professional conduct. U.S. attorneys open themselves up to liability if they do not or cannot adequately supervise the actions of foreign lawyers and non-lawyers to whom confidential client information is disclosed. The most effective way U.S. law firms and attorneys can protect themselves and their clients from ethical breaches are to enter

into a contract with the overseas company.[41]

Such a contract should set forth confidentiality and privacy responsibilities and restrictions. Overseas employees are expected to maintain the confidentiality of information relating to the representation of the client.[42] Outsourcing attorneys in the United States should take the time and effort necessary to ensure that foreign workers understand what the duty of confidentiality entails as well as its rules and application.[43] Offshore workers, for example, may not understand that the duty of confidentiality continues even after the project has been completed.[44]

The contract should provide the U.S. firm with confirmation that, not only do overseas workers understand their duties of confidentiality, "the outsource supplier has enforceable and enforced rules and procedures pertaining to the safeguarding of confidential information."[45] If the overseas employees are expected to protect client information under United States laws, such language should be included in the contract.[46] Educating overseas workers and binding employees at both ends through a contract will likely decrease both inadvertent and deliberate disclosures of confidential information.

C. Limited access to confidential information

The most practical and effective strategy to protect a client's privacy and prevent disclosure of confidential information may be to limit the outsourced worker's access to information. For document review services, for example, a law firm can utilize third party vendors that restrict access to secure documents only to those working on that particular issue. Vendors can also redact identifiable information, prevent copying and downloading of confidential material, and track access of confidential records.[47]

Limiting the outsourced worker's access to confidential client information is also beneficial for purposes of avoiding conflicts of interest. Screening overseas employees from all client information that is unrelated to their work on a matter helps prevent conflicts of interest for the U.S. attorneys and law firms.[48]

Many LPOs understand the importance of protecting confidential client information. LPO Atlas Legal Research, for example, "promises to thoroughly check for any potential conflict of interest and, at customer's request, will alter any personally identifying information before sending work assignment to India."[49] If overseas employees have limited access to confidential client information, the chances for unintentional or deliberate disclosure decrease dramatically.

V. Conclusion

The legal outsourcing industry is thriving. Offshore outsourcing of legal services offers decreased costs and increased efficiency, but it also raises ethical issues regarding a client's privacy and the duty to protect a client's confidentiality. U.S. law firms and attorneys can combat the dangers of inadvertent or deliberate disclosures of confidential client information in several ways. Attorneys must gain client consent for any offshore outsourcing. If they

decide to proceed with legal outsourcing, U.S. firms and LPOs should enter into contracts governing confidentiality obligations and restrictions. Limiting the outsourced worker's access to a client's confidential information can also have a significant impact on preserving client confidentiality. Outsourcing of legal services is not likely to slow down in the near future, so lawyers should take precautions to protect the client's confidential information and privacy.

---

[1] *See* Thomas L. Friedman, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY 137 (2d ed. 2006).

[2] *See* Mary C. Daly, *Flattening the World of Legal Services? The Ethical and Liability Minefields of Offshoring Legal and Law-Related Services*, 38 GEO. J. INT'L L. 401, 403 (2007).

[3] Alison M. Kadzik, *The Current Trend to Outsource Legal Work Abroad and the Ethical Issues Related to Such Practices*, 19 GEO. J. LEGAL ETHICS 731, 733 (2006).

[4] Daly, *supra* note 2, at 403.

[5] Lee A. Patterson, III, *Outsourcing of Legal Services: A Brief Survey of the Practice and the Minimal Impact of Protectionist Legislation*, 7 RICH. J. GLOBAL L. & BUS. 177, 182 (2008).

[6] *Id.*

[7] *See* Kadzik, *supra* note 3, at 733; Patterson, *supra* note 5, at 182; *See* ValueNotes, *Outsourcing in the Changing Marketplace*, http://www.sourcingnotes.com/content/view/667/92/ (last visited Dec. 5, 2010).

[8] *See* ValueNotes, *Outsourcing in the Changing Marketplace*, http://www.sourcingnotes.com/content/view/667/92/ (last visited Dec. 5, 2010).

[9] *Id.* Revenues may even surpass this number, as the industry is picking up pace as the global economy begins to recover.

[10] James I. Ham, *Ethical Considerations Relating to Outsourcing of Legal Services by Law Firms to Foreign Service Providers: Perspectives From the United States*, 27 PENN ST. INT'L L. REV. 323, 324 (2008).

[11] *Id.*

[12] Model Rules of Prof'l Conduct R. 1.6.

[13] Model Rules of Prof'l Conduct R. 1.6, cmt 16.

[14] Daly, *supra* note 2, at 436-437.

[15] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is one such federal law that may restrict who has access to a client's confidential information. Ham, *supra* note 10, at 334.

[16] Daly, *supra* note 2, at 438.

[17] Ham, *supra* note 10, at 335.

[18] Daly, *supra* note 2, at 438.

[19] *Id.* (Explaining that, "China and the Islamic countries where the shari'a is adopted…are certain to have radically different perspectives").

[20] Marcia L. Proctor, *Considerations in Outsourcing Legal Work*, 84 MICH. B. J. 20, 22 (2005).

[21] *Id.*

[22] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 at 5 (2008) (Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services).

[23] "For example, recently, an offshore subcontractor handling patient-record management for the University of California at San Francisco ("UCSF") Medical Center threatened to post confidential patient records on the internet unless the Medical Center straightened out a problem with the third-party vendor handling UCSF's accounts payable department. In another case, a Bangladore, India-based data manager held an American company's data hostage and refused to return it unless the American company dropped its legal claims against it." Ham, *supra* note 10, at 335.

[24] Daly, *supra* note 2, at 435-436.

[25] Steven C. Bennett, *The Ethics of Legal Outsourcing*, 36 N. KY. L. REV. 479, 482 (2009).

[26] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 at 2 (2008)

(Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services).
[27] *Id.*
[28] Model Rules of Prof'l Conduct R. 5.1(b).
[29] Model Rules of Prof'l Conduct R. 5.3.
[30]ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 at 3 (2008) (Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services).
[31] *Id.*
[32] *Id.*
[33] *Id.* at 4.
[34] Gabe Acevedo, *Legal Olympics Update: Outsourcing E-Discovery Sliding Down Slippery Slope, at Record Speed*, Feb. 16 2010 http://abovethelaw.com/2010/02/legal-olympics-update-outsourcing-e-discovery-sliding-down-slippery-slope-at-record-speed/ (last visited Nov. 25, 2010).
[35] *Id.* According to Gabe Acevedo at "Above the Law," some firms have already found themselves in similar situations.
[36] The committee opined that, "when a lawyer engaged the services of a temporary lawyer, a form of outsourcing, an obligation to advise the client of that fact and to seek the client's consent would arise if the temporary lawyer was to perform independent work for the client without the close supervision of the hiring lawyer or another lawyer associated with her firm." ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 at 4 (2008) (Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services), *citing* ABA Comm. on Ethics and Prof'l Responsibility Formal Op. 88-356 (Dec. 16, 1988) (Temporary Lawyers).
[37] Explaining that such a situation "ordinarily will not be the case in an outsourcing relationship, particularly in a relationship involving outsourcing through an intermediary that itself has the employment relationship with the lawyers or nonlawyers in question." ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 at 5 (2008) (Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services).
[38] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 at 5 (2008) (Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services). (citing Model Rules of Prof'l Conduct R. 1.6 (a), 1.6 cmt. 5 (2008)).
[39] Patterson *supra* note 5, at 188.
[40] *Id.* at 193.
[41] Ham, *supra* note 10, at 325.
[42] Kadzik, *supra* note 3, at 736.
[43] Ham, *supra* note 10, at 336.
[44] Daly, *supra* note 2, at 438.
[45] Ham, *supra* note 10, at 336.
[46] Proctor, *supra* note 20, at 22.
[47] Ham, *supra* note 10, at 337.
[48] Kadzik, *supra* note 3, at 735.
[49] http://www.atlaslegal.com/ Atlas Legal Research, http://www.atlaslegal.com/ (last visited Nov. 29, 2010).

The Judgment of Google

By Valerio Vallefuoco

Valerio Vallefuoco is a managing partner with Studio Legale Vallefuoco & Associati in Rome, Italy. He concentrates his practice of law in commercial litigation, European and international law. Currently, he is a professor of international tax law at the Lum Jean Monnet University in Italy.

ON THE 24 February 2010, judgement was entered, and defendants Drummond De Los Reyes, Google's senior vice president of corporate development, Peter Fleischer, global privacy counsel, and George Reyes, a former chief financial officer, were convicted, as a result of a video that appeared on the Google Video site portraying an autistic person being beaten by his classmates at a school on the outskirts of Turin. Prosecutors in Milan brought charges after an appropriate and complete investigation. The individuals mentioned above were accused of the crimes of defamation and dissemination of sensitive information without proper authorization.

The events in question occurred in a public school where there were a number of youths with their autistic companion. The commentary on the video shows one of the youths making a mocking call to the "Vivi Down" charity, and Vivi Down was the civil party asserting the crime of defamation during the criminal proceedings.

It goes without saying that the story had a huge media following, not only because of the importance of the parties concerned, but also because the sentence could have been in one way or another a precedent for or against those who own websites and are involved in the uploading and downloading of information continuously from users who surf the web.

The proceedings also had a huge media following because of the cruel facts, the identity and status of the victim, and the fact that the youths of the video wanted to make public their vile behaviour. Since then, interest has grown in part because of the implication of the most powerful and well known search engine in the world, Google, and its possible liability.

The issue concerning the removal of defamatory content on web space provided by Google has been a rather tricky subject in the past. For example, the decision of the Supreme Court of New York, which issued a ruling in favor of Canadian model Liskula Cohen and ordered Google turn over the name of an anonymous blogger so that Cohen could pursue a lawsuit against the blogger for defamation. The plaintiff also asked the court for the removal of all content from the sites. It took just under a year, but eventually Cohen succeeded in forcing the most popular search engine in the world to reveal the identity of the anonymous Internet user. This case illuminates an important issue concerning people who choose to abuse the freedom

provided by the Internet and its anonymity and their obligation to answer for any revelation of private, sensitive information.

The case in Milan involved allegations against the directors relating to the defamation of the charity "Vivi Down" and the beating of the boy, Mr. De Leon. The allegations involved harm to the interests of people who had not given their consent for the processing of information entered into the system which was used by Google to produce profits. The technical and legal connections involving the search engine in question have been thoroughly explained before and leave no doubt as to the conduct of the same American company.

The relevant charges specifically involved: 1) Complicity of the defendants in defamation, having contributed to the defamation of the “Vivi Down” charity by the implementation of omissive behavior (the defendants failed to either do something to solve the situation, warn those who controlled the uploaded videos or to try to change the rule to prevent internet users from uploading such videos) and 2) benefiting from the disclosure of personal information about a person without permission.

As is easy to understand, the interests at stake are not only related to one of the largest corporations in the world, but also to the millions of people every day that are on the net. We must assume that there is no universal specific legislation on the rules to be followed in carrying out activities on the web, and that the rules being used are derived from laws created in other areas which also apply in this media world that every day is becoming more prominent in our daily life. It is only logical that these legislative gaps cannot be filled so easily, but they must be recorded and resolved one by one, to ensure that there is no doubt or inconsistency in the application of one rule to another.

Article 595 of the Italian Criminal Code states the crime of defamation: “Anyone, except for cases mentioned in the previous article, communicating to more people, injures another's reputation, shall be punished with imprisonment of up to one year or a fine of up to € 1032. If the offence concerns the attribution of a given fact, the penalty is imprisonment for up to two years or a fine of up to € 2065. If the offence went through the press or any other means of publicity, or in a public deed, the punishment shall be from six months to three years imprisonment or a fine of no less than € 516. If the offence went to a political, administrative or judicial body, or any of its representative offices, or by a panel authorities, the penalties are increased.”

In this case, the imputations are flanked by another behavior, identified in Article 40 of the Italian Criminal Code, which requires verifying a well-defined behaviour: failing in forbidding a criminal action is tantamount as causing it. The Court found that there was not enough sufficient evidence of the behaviour of the defendant by the prosecution, and therefore the defendants were found innocent under Art. 40.

Above all, we must consider that the defendants did not deny that the defamation occurred, and the Judge ruled that the owners of the site could not be held responsible for the crime, as it was not intended. Specifically, the youths in the video portrayed themselves as being

part of "Vivi Down," and that portrayal and the associated comments not only defamed the company in question, but also affected the whole world in connection with Down syndrome.

The reason that prompted the jury to acquit the accused on the first charge was the fact that the charges, as proposed required a prior or subsequent control of the information entered into the site video.google, but this control, in the Court's opinion, was impossible to exercise. Preventive control was not possible if attempted, because it would effectively block the use of Google due to the amount of information uploaded by users of the Web at any time. The control needed in another level, however, as suggested by the prosecution is not required given the lack of specific legislation governing its activities According to the Public Prosecutor, the failure of control occurred after the release of information into the system, which would have warned them of the offence, and it would not have happened (or would have happened but with less harm to the victim).

This assumption, however, is not provable because even if there had been a follow-up, the fact remains that it could have still passed unnoticed, given the thousands of videos uploaded daily on the site. However, it is vital to understand how the PM has come to challenge the offence of defamation by the administrators and Google Italy Google Inc. The fundamental distinction that involves the Google administrators on the witness stand relates to the difference between content providers (content management system) and host providers (third party liability).

If the video.google site was considered by the Court to be a simple host provider, the problem on the liability part and the allegations in question would not even be up for discussion, but the Prosecutor's investigations revealed that the site, although it is free, does not merely allow the user to upload or download videos, but handles them, without screening their content. This difference has placed the site in a very awkward position, because Google has become complicit in the dissemination of information uploaded by a third person, even if the information is made public without proper authorization.

In fact, the sentence on the first charge of the indictment does not say that Google Italy, and therefore the accused, did not commit the fact, but ruled instead that the indictment provides as follows: expected behaviour that administrators should have taken but was impossible to apply, because the control needed would have made it impossible for the service rendered. Therefore if Google was applying the level of control the Prosecutor wanted, no service would have been provided at all. If the site had been considered a simple video.google host provider, then there would have be no charges against the administrators who run the company (at least in Italy).

The fact that the site has been identified as a content provider poses a different question. The prosecution did not prevail only because prevention control was not possible in this case in question. Furthermore, the construction of a position of security requires the person against whom is entrusted with an obligation "quote" to prevent the event and not a general obligation to make an

end to the effects occurred. This means that the obligation is fulfilled the moment that the internet user tries to prevent the event, but if for any reason such event occurs, then it is not longer his obligation to end it. (Given the extreme technical difficulty of this solution and the consequences that might ensue, it would be viewed as an "unreasonable" requirement and therefore not criminally liable under Article 40 of the Italian criminal code.)

On the other hand, the second indictment involves the processing of personal data of De Leon. This second charge is rooted in the fact that the video.google site in Italy for which Google Inc. is responsible is considered, as mentioned before, a content provider, i.e. a site that is not just a passive intermediary, but that manages the information that is entered into their system. The article in reference to this charge is Article 167 of the Privacy Law, which states that:

> "1. Unless the act constitutes a serious crime, whoever, in order to gain profit for himself or others or to cause harm to others, must not process personal data in violation of the provisions of Articles 18, 19, 23, 123, 126 and 130, or Article 129, shall be punished, if harm comes from the fact, with imprisonment from six to eighteen months or, if the fact consists in communication or dissemination, by imprisonment from six to twenty-four months. 2. Unless the act constitutes a serious crime, whoever, in order to gain profit for himself or others or to cause harm to others, must not process personal data in violation of the provisions of Articles 17, 20, 21, 22, paragraphs 8 and 11, 25, 26, 27 and 45, shall be punished, if harm comes from the fact, with imprisonment from one to three years."[1]

The prosecution therefore had to demonstrate the link between Google Inc. and its representative company in Italy, Google Italy, in the management of a site apparently free to users, but that is a source of income. The site which was used to "load" the video in question allows any registered user to enter any kind of (video) information in the system with the only filter being a flag-in on the privacy law. In the jury's opinion, this was a completely inappropriate way to inform users on the law of privacy. The information that is "loaded" on the site is managed by Google, although in an autonomous way: the video, depending on the number of downloads is placed in a ranking, then the same is put into a category, so that the site handles the information and advises users, offering one video instead of another. In fact, if a video is entered into this website, it then places it among the top in the category of funny videos, invariably the operator of the website recommends watching that video to users.

In the case in question, the Prosecutor of Milan found that the accused Drummond, De Los Reyes and Fleisher, in their individual capacity as officers, (the first two from Google Italy and the third from Google Inc.) in relation to the privacy policy for Europe, committed the crime in question by failing to properly handle personal data and sensitive information of Giovanni Francesco De Leon, allowing the loading

of the video file on September 8, 2006 and maintaining it on the Google video.it site in order to make a profit. This profit, according to the prosecution derives from the relationship between Google Italy with the video.google site and operations on the same site of the AdWords system.

This system, in short, allows anyone who wants to advertise to have their advertisements seen when the most successful videos are downloaded. So if the company "Acme" wants to advertise on the most downloaded video of the moment, it pays to make its site have a link with the video. In such a case, the requirement of the second aspect of the configuration provided by Art. 167 of the Privacy Act would be met, namely the profit.

Based on this interpretation, where substantiated by the facts, those responsible for the site should therefore be held jointly responsible for the offence under Art. 167 because this kind of ISP (website) not only provides a simple report of interconnection, but also manages data in its possession, such that it becomes somehow "dominus" and then "the data controller" in accordance to law with corresponding obligations.

While confirming what was previously said, one cannot ask the content provider to perform prior checking on the information entered into the system, it is possible, and even necessary, to ask the provider to meet another kind of obligation: the operator of the site which enables users to "load" the video's on the video.google domain must have correct information and must comply with the consequent obligations imposed by the same law, or the operator runs the risk of non-compliance (the immediate cancellation of data and communications and a report of criminal activity).

Accordingly, the Court considered it insufficient to meet the requirements of the law "to hide" the information on these obligations within the general conditions of the service accepted at the time of registration of the user for use of the service. Thus, in fact, the Judge was not satisfied with the knowledge that every user should have to respect, giving due weight to this statement, among other things, not being informed about the consequences that could arise if the user does not comply with the law. In light of these facts, the directors of Google Inc. and Google Italy were found guilty of the second part of charge ascribed.

Other factors helped to strengthen the argument of the prosecution. Research of the accused has shown that Google Inc. operates in all respects for Google Italia from a commercial entity, Google Italy. For any type of decision Google Italy must request permission from Mountain View, based in the United States. This does not mean that the company Google Italy Srl cannot exist without the administrators, even if nominally and formally responsible for the company. Investigations have shown specifically a lack of respect for the Italian law and at the same time the enormous difficulties in the operation of the company in dealing with priority needs, which was reflected in the choice of the Administrators.

The continuing need to ask authorisation for every modification, request or problem can halt the normal activities of the company, to the extent that Google Inc. and Google Italy often had to pay penalties in compliance for

late entry in the book of records of business. Specifically, administrators and heads of Google Italy, selected by American leadership, had management problems arising out of unawareness about the national legislation. Because the Defendants were not Italians, they found themselves in a somewhat awkward situation: they are formally responsible as they are the legal entities involved in the management of the company concerned, but investigations revealed that the internal structure of Google Inc. is vertical, and that all decisions are made in Mountain View. No one responsible had ever bothered to raise the issue concerning the privacy of users or those using the service rendered by video.google, or bothered to change the privacy statement at the time of the service or to apply for permission to Google Inc. to adapt the announcement of conditions of privacy found only on the general conditions of service.

The directors, as such, should deal with the company as if it were really them, that is, controlling all the aspects that can put the company in unpleasant situations. In this writer's view, the directors have borne the brunt of the complicated corporate management of Google Inc. who personally manage every decision, something completely unthinkable given the volume of the company. The conduct of the directors to manage or to "pretend" to manage a very complex society that not only provides some occasional signature, but needs much more attention than an ordinary company, not only due to the fact of the sensitivity of information handled, but also because of the number of users who access the service every day, shows the trust placed in the parent company was misplaced.

Administrators like it or not, are responsible for everything that happens within the company they represent, and it does not matter if one is part of a larger company. In this case the defendants have the sin of superficiality, because their named positions mandated their responsibility from legal point of view. It is unthinkable that the volume of management decisions in a large or small company can be handled by a person who does not fully know the issues relating to relevant accounting and legal principles. Moreover, the growing daily relations with users of a service with a higher power of information than television and other media must be approached with care and dedication, which the directors of Google Italy did not do. The result was that the directors have had to bear responsibility for their choices.

Naturally we must keep in mind the position of the accused within the company to fully understand the nature of the charges against them. Italian Civil Code Art. 2392 identifies the responsibilities of directors to the company. The article stipulates that "those who occupy a post of senior management have an obligation to fulfil duties imposed by law and by statute, with the diligence required by the nature of the assignment." There does not appear to be any problem from this provision, but in this case, from the corporate structure of Google and the administrative positions they held, the defendants have been put in a position where they have to be responsible for everything that concerns corporate activity, especially in a unique company

which continuously manages hundreds of thousands of items of sensitive information. The directors' behavior, as shown by the evidence adduced by the prosecution, was not exemplary. Although the defendants, in different ways have shown that they have never really been aware of what "their" company did. Therefore, when the video in issue was uploaded to the site, it put the U.S. search engine in an uncomfortable situation of control. As a result, control was not sufficiently performed by anyone. Indeed, the fact that it categorized the video as "more fun" just worsened the situation for Google and its directors who failed to exercise the necessary control. In this regard, Art. 40 of the Italian Criminal Code states, "He who does not prevent an event who has a legal duty to do so, amounts to cause."

The obligation of directors, individually and separately, derives from their designated positions within the company. In theory, they should have controlled the relevant company operations, no matter who was in Mountain View, because ultimately, from a legal point of view, they and they alone had the responsibility. The Italian doctrine defines this position as "position of guarantee," where the charge of a particular person is created to avoid situations in violation of law. In this respect Article 41 of the Italian Constitution was also involved, granting freedom of economic initiative and implicitly recognizing that it is the holders of the initiative (profiting from it) that have to provide adequate organizational security for the interests protected.

The doctrine would provide a logical solution to address a problem of any director belonging to large media companies: The law allows an administrator responsible the use of "delegation" where they cannot "see". A defence of delegation was previously weakened by the prosecution from the evidence sought by the Prosecutor. Several people from Google Inc. and Google Srl were called to testify only to say that no one had been delegated to deal with the problem directly. The evidence not only showed that the management of the company was only nominally in the hands of the defendants, but also demonstrated that the operation carried out by Mountain View was not adequate.

The ruling was proof that even in the absence of a law degree, despite the changes to the facts that every day change and update, the rules can, although with some difficulty, be applied to new situations that arise each day. In fact, even if the law cannot update on real time (in this case, represented by many different situations), we clearly see that today it is still possible to apply old solutions to the present problems.

The significance of Google's media decision certainly was a wake-up call, not only for operators of the website, but also for large companies that tend to centralize the control of "affiliated entities" in their own hands in the manner of Google Inc.

Surely by now all the operators of sites, blogs or general information should monitor the space they make available on the network. This ruling confirms that he is punished who benefits from the incorrect behaviour of another person. It is necessary that the operator does not

contribute to spreading the wrong message by neglect or omission. In this respect it is the exemplary remarks made by the Judicial body, which, in the expectation and hope there could soon be a good law formulated for governing such situations, stated, using a famous Latin sentence, that there is no worse dictatorship than that exercised in the name of absolute freedom, "legum servi esse debemus, ut liberi esse possumus."

---

[1] DL 196/03.

Privacy Please: How Companies Should Navigate Strict Foreign Privacy Laws in Today's Global Economy

By: Kyle Dreyer, Wendy May and Joy Tull

SINCE the expansion of sweeping American-style discovery over the last several decades, foreign countries have enacted privacy laws in an effort to prevent or severely limit United States (U.S.) litigants and courts from obtaining otherwise discoverable but private materials from within the borders of foreign countries.[1] Foreign privacy laws generally restrict both foreign and domestic entities from reviewing, collecting or disseminating personal information, defined as any information relating to an identifiable individual.[2] However, the privacy often treated as sacrosanct by foreign countries, has long been discounted by U.S. courts. Traditionally, perhaps pressured by the tenant of open discovery, U.S. courts have acknowledged the existence of foreign privacy laws but have not recognized these laws as a barrier against broad form orders requiring production of information collected and maintained abroad. U.S. courts have consistently determined domestic litigants'[3] interest in full disclosure should prevail over foreign privacy interests.[4]

Adding to the conflict, the European Union (EU) and member countries have begun using their newfound power to strengthen privacy protection enforcement, including criminal penalties actually imposed on privacy law violators.[5] In this increasingly global economy, U.S. litigants with foreign subsidiaries or affiliates may be forced to choose between potential sanctions by a U.S. court for non-production or the consequences imposed by a foreign country for violating privacy laws.[6] Recognizing this dilemma, some recent U.S. rulings have signaled a shift toward genuine consideration of foreign privacy interests. However, U.S. courts are far from consistent in their protection of private foreign information. Until they are, U.S. litigants should be prepared to protect against the increased risk of penalties for privacy law violations.

Kyle H. Dreyer and Wendy D. May are partners with Hartline Dacus Barger Dreyer LLP in Dallas, Texas. Mr. Dreyer's practice areas include complex product liability, commercial and malpractice litigation.

Ms. May concentrates her practice in the areas of complex product liability and commercial litigation.

Joy R. Tull is an associate in the Dallas office and practices in the same areas.

I. Foreign Privacy Laws and the Impetus for Increased Enforcement

A generalized disdain for the broad pretrial discovery process allowed in the United States is well-documented abroad.[7] Foreign privacy laws have long existed and included criminal sanctions as

penalties for those who disseminate protected private information. Nonetheless, litigants who produce protected private information in response to U.S. court-ordered production have not been prosecuted in the past. Recently, however, foreign jurisdictions have begun enforcing criminal penalties against U.S. litigants and their foreign affiliates for privacy law violations. [8] Since countries throughout the world have privacy laws that have been largely dormant until now, it is necessary to understand the catalyst for increased regulations and enforcement in order to predict which countries this trend may next reach.

A. Geopolitical Changes

Although the EU has existed in various forms since 1948, its current economic and political powers have increased over the last 20 years and particularly since 1995.[9] Relying on its enhanced power and influence, the EU's Parliament and Council drafted a set of regulatory directives for enactment by individual EU member countries as domestic law.[10] One EU directive, Directive 95/46/EC (the "Privacy Directive"), requires member countries to protect the privacy rights of individual citizens through legislation.[11] Compliance with this directive requires member countries without privacy laws to pass and enforce them and member countries with privacy protection laws to more strictly enforce them.[12] France is one example of an EU member country with longstanding privacy laws, which has recently increased enforcement. France's privacy laws were enacted in 1974 but the criminal penalties permitted were not sought against those responding to U.S. discovery requests until 2007.[13] Other EU countries have since followed suit, as exemplified by Italy's imposition of criminal sanctions against three Google executives for violating the country's privacy restrictions.[14]

B. Impact of the Patriot Act

The widespread adoption of the Privacy Directives by EU member countries, as well as the increased willingness of these countries to enforce their respective pre-existing privacy laws, may represent a response to international sensitivity over the U.S. Patriot Act[15] passed in 2001. The Patriot Act is seen by foreign leadership as the latest and perhaps most egregious step toward undermining EU citizens' privacy rights.[16] And, EU member countries have responded, in part, to U.S. enforcement of the Patriot Act with the first criminal sanctions imposed under pre-existing privacy laws.[17]

C. Increased Electronic Data

Another trigger for recent foreign privacy law enforcement is the exponential increase in private information now available electronically. Simply put, far more personal data is now collected, stored, and accessible due to the increased capacity afforded by digital processes. Moreover, much potentially private information can exist with non-protected data but be hidden in the metadata or electronically stored information (ESI). Thus, foreign countries see increased restrictions as necessary to prevent dissemination of

private information accessible in ESI files.

II. U.S. Court Response to Foreign Privacy Law Enforcement

The Hague Convention on the Discovery of Evidence Abroad (the "Hague Convention") is one method utilized by U.S. litigants to avoid violating foreign laws during the discovery process.[18] The Hague Convention is intended, in part, to ensure that foreign privacy laws are not violated while allowing U.S. litigants to obtain discovery of information located abroad.[19] However, U.S. courts have often criticized Hague Convention procedures and generally opposed using them.[20] U.S. litigants found justification for bypassing the Convention's procedures altogether[21] in the Supreme Court's *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa* analysis.[22] While the *Aerospatiale* Court adopted a test to weigh foreign privacy interests against domestic discovery interests, in its application by U.S. courts, this five-factor comity analysis has historically amounted to little more than token recognition of foreign privacy laws. In fact, U.S. courts have frequently refused to temper discovery orders that may potentially violate such privacy laws.[23]

However, the EU Privacy Directives, and the more robust privacy law enforcement by foreign countries generally, have recently begun to impact the application of both the *Aerospatiale* comity analysis and the Hague Convention procedures by U.S. courts. In the past, litigants were not guaranteed the court would recognize the Hague Convention as a valid solution to foreign discovery issues; much less seriously consider the threat of foreign prosecution.[24] Now, outcomes in cross-border discovery disputes range from applying all five comity factors and finding in favor of foreign privacy interests, to at least a willingness to consider the protections offered by the Hague. [25]

In the few U.S. cases decided after France first began imposing criminal sanctions for privacy law violations, U.S. courts have incorporated into their application of *Aerospatiale* a more thorough evaluation of specific foreign privacy interests. Specifically, these courts have focused on whether U.S. litigants or their foreign affiliates realistically face a risk of foreign prosecution for complying with a particular discovery request and how vigorously the foreign jurisdiction defends its own privacy laws.[26]

For example, in *Gucci Am., Inc. v. Curveal Fashion*, the United States District Court for the Southern District of New York, recognized that criminal sanctions authorized by Malaysian privacy laws "suggest that Malaysia has a strong [privacy] interest" demanding some consideration by U.S. courts.[27] However, because the Malaysian government had made little previous effort to enforce its privacy laws, and no effort at all to intervene in the case, the *Gucci* Court ultimately did not limit discovery.[28] The Court appeared to affirm on the basis that without an actual danger of prosecution or objection by the foreign government, there was no basis for protecting Malaysian privacy interests

over the U.S. discovery interest.[29] During the same month, in *In re Air Cargo*, the United States District Court for the Eastern District of New York utilized a similar analysis, considering both the realistic risk of prosecution based on case specific circumstances and the efforts of the French government to enforce its privacy laws.[30] The thorough analysis and genuine consideration given the *Aerospatiale* comity analysis by both the *Gucci* and *In re Air Cargo* courts represents deference given to foreign privacy interests that was previously very hard to come by.

Although both *Gucci* and *In re Air Cargo* resulted in ordered discovery that could potentially violate international law, the decisions were premised on fact specific circumstances that are not necessarily applicable to other foreign countries. For instance, Malaysia is neither a member of the EU nor a signatory to the Hague Convention, therefore the U.S. court discounted the foreign privacy interests implicated. In *In re Air Cargo*, the documents at issue had previously been produced with the permission of the French government in another matter; prompting the Court to question the seriousness of the privacy concerns raised.[31]

U.S. Courts have also begun to reassess the appropriateness of the Hague Convention procedures in certain circumstances. For example, in *Motorola Credit Corp. v. Uzon*, the United States District Court for the Southern District of New York refused to compel a bank to produce information, based in part, on the requesting party's failure to follow the Hague Convention procedures.[32] The U.S. District Court for the Eastern District of Michigan authorized the use of the Hague Convention procedures, even though the procedures are "more difficult and more expensive" than those provided in the Federal Rules of Civil Procedure.[33]

By careful application of the *Aerospatiale* factors and authorizing the use of the Hague Convention procedures, U.S. courts are allowing foreign countries to have some greater measure of control and protection over the interests of their citizens' personal privacy during the U.S. discovery process. Even recognizing the fact specific outcomes in the above referenced cases, the general privacy protection represented by them suggests a trend toward increasing concern for foreign privacy interests. U.S. litigants faced with the challenge of responding to requests for the production of foreign private information must demonstrate that the foreign country's privacy interests warrant serious concern, based in part on the country's privacy law enforcement history. Additionally, parties should not overlook the potential benefits of seeking authorization for the use of the Hauge Convention procedures, as well as intervention from the foreign country at issue.[34] Letters from foreign ambassadors and foreign judicial officials have been enough to convince some courts that relief from U.S. discovery demands is in order.[35] At the least, when faced with foreign privacy interest laws, the Hague can and should be used to allow the foreign country to assert its interests.[36]

III. How to Avoid Entanglement in the Conflict

While there is a shift toward carefully considering and even restricting discovery of foreign protected private information, it is left to individual courts to balance the competing interests.[37] Thus, a consistent approach has not yet developed.

The EU's Privacy Directives protects a broad spectrum of "personal data," defined as any information relating to an identifiable individual.[38] This means any information even tangentially related to an individuals' specific physical, physiological, mental, economic, cultural, or social identity as well as anything suggesting financial information, organizational affiliations, racial or ethnic identity, health status, email address, or phone number is protected by law.[39] This protected information is not only included in many discoverable documents requested in litigation, but is also often acquired for statistical analysis and research. Thus, U.S. entities must consider how this protected information should be handled both inside and outside the U.S. litigation context. U.S. companies which are involved in litigation, or which may use this type of information for other business purposes, should be cognizant of both applicable foreign privacy laws and the still inconsistent protection offered by U.S. courts. To that end, the following considerations are significant: (1) identifying foreign relationships that may create access to private protected information, (2) knowing the law and enforcement history in those foreign jurisdictions where those relationships exist, and (3) adopting document retention and document management policies that comply with applicable foreign privacy laws.

A. Identify Relationships with Foreign Entities that Create Access to Private Information

U.S. entities risking conflict with foreign privacy laws are those that seek private information 1) pursuant to discovery requests; or 2) for internal uses like research and statistical analysis. U.S. discovery rules only require a party to produce relevant information within its possession, custody, and control.[40] This requirement is generally interpreted to include all such material held by any entity over whom the party has a right to compel production.[41] Typically, this includes wholly or partially owned foreign subsidiaries or affiliates, foreign-owned parents, and potentially foreign-owned suppliers.[42] Thus, only those U.S. entities with qualified foreign affiliates risk a discovery scenario where foreign privacy laws conflict with U.S. discovery obligations. Likewise, any U.S. entity using a foreign affiliate (even if not "controlled" by the U.S. entity) to collect statistical data for research and analysis should consider the potential application of foreign privacy laws before obtaining any potentially private information.

B. Understand the Law and Enforcement Policies in Applicable Foreign Jurisdictions

Once potentially problematic foreign affiliates are identified, it is important to understand the nuances of privacy law and the penalties imposed in each

particular foreign jurisdiction. While the EU Privacy Directive provided the framework for a more unified approach, each member country is free to enact its own specific privacy laws and, of course, these vary. Not every foreign jurisdiction has shown an equal willingness to enforce its privacy laws and some have even provided "safe harbors" for accessing private information.[43]

C. Effectively Manage Private Information

Assuming a qualifying foreign relationship exists where privacy laws restrict information commonly requested in discovery or used for business purposes, is it advisable to develop a compliant document retention policy. In the normal course of business, U.S. entities should not take actual possession of foreign protected information. Moreover, foreign subsidiaries, parents, and possibly suppliers of U.S. entities should also abstain from collecting, maintaining or reviewing personal information, even within their own borders.[44] If a company consistently applies and enforces document retention policies that exclude private information, U.S. courts have been more willing to defer to those policies when considering discovery objections.[45]

While the ideal solution is to avoid collecting or retaining protected information, that is not always realistic. Because entities based in countries with privacy restrictions are in the best position to avoid violating them, they may be better positioned to review and redact information when transfers of protected information are necessary. In some foreign jurisdictions, domestic entities can obtain consent from the relevant parties allowing them to collect personal data without violating applicable privacy laws.[46] However, such consent often does not translate to U.S. based operations.[47] When it is necessary to obtain information that may include private data, U.S. entities should protect themselves by requiring the foreign entity to redact private information before accepting a transfer.[48] By placing the burden of reviewing and censoring the information on the foreign entity, questionable material can be removed in compliance with applicable foreign privacy laws.

The easiest mistake for U.S. entities to make in regard to foreign privacy laws is a product of modern technology: neglecting to give electronic information the same, if not more, protection than that given to tangible documents and information. Foreign privacy laws prohibit corporations and other entities from storing, accessing, reviewing, or even organizing e-data covered by such privacy laws.[49] The Federal Rules of Civil Procedure have allowed for e-discovery since 1970.[50] However, many U.S. courts have more recently adopted stricter production requirements for electronic discovery.[51]

The EU Privacy Directives forbid storing or maintaining personal information, regardless of whether such would constitute spoliation in a U.S. court.[52] This heightened burden, from both sides, combined with the increased amount of data that now exists electronically, makes the risk for privacy violation more substantial.[53] As discussed, digital documents can contain a massive amount of unseen ESI that exists mostly in the background of

electronic transfers. Thus, it is easy to exclude ESI from the review and redaction process. The potential result is obtaining carefully reviewed and edited information that inadvertently includes personal data in the attached ESI. Should a company neglect to address ESI, it may be forced to preserve and produce the information it has received.[54]

As discovery in U.S. civil actions is increasingly impacted by shifts in foreign privacy laws and technological advancements, U.S. courts have indicated a willingness to consider the privacy challenges faced by U.S. litigants. Through careful attention to the protections offered by older tools like the Hague Convention and newer tools like the EU Privacy Directives, U.S. litigants can often find protection for their privacy interests in U.S. courts. Better still, careful document use, retention and storage planning may allow U.S. litigants to avoid privacy and disclosure conflicts before they arise.

---

[1] *See, e.g.*, Law No. 80-538 of July 16, 1980, Journal Officiel de la République Française [J.O.] [Official Gazette of France], July 17, 1980, p. 1799 (French blocking statute); Strafgesetzbuch [StGB] [Criminal Code] Nov. 8, 1934, art. 271 (Swiss blocking statute). For the sake of time and space this article refers to privacy laws generally and should be understood to include blocking statutes.

[2] *See* European Commission, Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN (2007), available at http://eur-lex.europa.eu/en/index.htm (last visited October 28, 2010); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002 P. 0037 – 0047 available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML; *see also* Privacy Directive, *infra* note 11, art. 2(a) ("an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or . . . one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.*

[3] While this article addresses the conflict for U.S. based companies with access to private foreign information, the same concerns and analysis offered here, apply equally to foreign entities subject to U.S. court jurisdiction.

[4] *See, e.g.*, Valois of Am., Inc. v. Risdon Corp., 183 F.R.D. 344, 346 (D. Conn. 1997) ("In many of the post-*Societe Nationale* decisions, . . . judges were unwilling to attach much significance to the sovereign interests involved, finding no important interest to be offended by use of the Federal Rules, and instead recognized that use of the Hague Convention could involve considerable time and expense.").

[5] *See* Cour de Cassation chamber criminelle [Cass. Crim.][highest court of ordinary jurisdiction] Paris, December 12, 2007, Bull. crim., Appeal n 07-83228 (fining "Christopher X" €10,000 in part for violation of a French blocking statute in connection with discovery in a U.S. case); Adam Liptak, *When American and European Ideas of Privacy Collide*, N.Y. TIMES, Feb. 27, 2010, available at http://www.nytimes.com/2010/02/28/weekinre

view/28liptak.html (discussing Italian courts' enforcing criminal sanctions against Google executive for violating privacy laws); Marc Gottridge and Thomas Rouhette, *France Puts Some Muscle Behind Its Blocking Statute*, 239 N.Y.L.J. 82 (2008).

[6] *See* M. James Daley & Kenneth N. Rashbaum, THE SEDONA CONFERENCE, A FRAMEWORK FOR ANALYSIS OF CROSS BORDER DISCOVERY CONFLICTS: A PRACTICAL GUIDE TO NAVIGATING THE COMPETING CURRENTS OF INTERNATIONAL DATA PRIVACY AND E-DISCOVERY 1 (2008).

[7] *See, e.g.*, Radio Corp. of Am. v. Rauland Corp., [1956] 1 Q.B. 618, 643-44 (describing the American pre-trial process as the "almost abusive discovery permitted by American law.").

[8] *See* Cour de Cassation chamber criminelle [Cass. Crim.] Paris, December 12, 2007, Bull. crim., Appeal n 07-83228.

[9] DIRECTORATE GENERAL FOR ENLARGEMENT, UNDERSTANDING ENLARGEMENT: THE EUROPEAN UNION'S ENLARGEMENT POLICY, 16 EU Publications Office (2007), available at http://www.delmkd.ec.europa.eu/en/broshures_and_campaigns/Undestranding%20Enlargement%20EN.pdf. Since 1995, European Union membership has increased from 12 to 27 countries, providing the European Union with the combined negotiating power and economic influence of industrialized nation status in Western and Eastern Europe. *See* KEY ASPECTS OF GERMAN BUSINESS LAW 422 (Bernard Buecker et al. eds., 3rd ed., Springer, 2006). Indeed, since its introduction in 1999, the Euro has become the second largest reserve currency and second most traded currency in the world – second only to the dollar. *See* Aleksander Aristovnik & Cec Tanja, *Compositional Analysis of Foreign Currency Reserves in the 1999-2007 Period. The Euro v. The Dollar as Leading Reserve Currency*, 13(1) J. FOR ECON. FORECASTING 165-181 (2007).

[10] *See, e.g.*, Council Directive 95/46/EC, 1995 O.J. (L 281) 31-50 available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[11] *See id.* [hereinafter Privacy Directive]. The privacy directive encourages members states to protect "the right to privacy" while still providing for differences in the "variety of national laws, regulations, and administrative provisions." *Id.* at (7).

[12] *See, e.g.*, Federal Act on Data Protection ("BDSG") January 27, 1977 (*Bundesgesetzblatt*, Part I, No 7, February 1, 1977), amended in 1990. Privacy & Human Rights 2003, An International Survey of Privacy Laws and Development, Federal Republic of Germany, FN 1182, available at http://www.privacyinternational.org/survey/phr2003/countries/germany.htm. Germany is one of many European Union members which had to revise pre-existing privacy laws, in place since 1974 to comply with the new EU Directive. *See id.* Once the EU Directive passed, Germany was forced to refine its privacy restrictions to comply with the stricter requirements of the new Directive. *Id.*

[13] *See* Cour de Cassation chamber criminelle [Cass. Crim.] Paris, December 12, 2007, Bull. crim., Appeal n 07-83228. This case is one example of increased enforcement of privacy restrictions by EU countries, in response to discovery requests from U.S. litigants.

[14] Adam Liptak, *When American and European Ideas of Privacy Collide*, N.Y. TIMES, Feb. 27, 2010, available at http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html; John Hooper, *Google Executives Convicted in Italy*, THE GUARDIAN,

Feb. 24, 2010, available at http://www.guardian.co.uk/technology/2010/feb/24/google-video-italy-privacy-convictions. Although this conviction was not directly tied to United States' discovery efforts to obtain information located abroad, it does strongly suggest the European community will not hesitate to enforce its privacy laws through criminal penalties and/or sanctions against those who provide or produce private information protected by statute.

[15] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 18 USC § 2712, 31 USC § 5318A (2004). The statute is commonly referred to as the "Patriot Act". *Id.*

[16] *See e.g.*, Justin Santolli, *The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Privacy Directive*, Note, 40 GEO. WASH. INT'L L. REV. 553 (2008) (suggesting the EU's response to the Patriot Act was to pass additional privacy protections in the face of what is widely viewed in the EU as overreaching by the U.S. government); Dan Bilefky, *Europeans Berate Bank Group and Overseer for U.S. Access to Data*, N.Y. TIMES, Oct. 5, 2006, at A15 (documenting the European Parliament's criticism of U.S. access to banking information pursuant to the Patriot Act).

[17] *See* Gottridge & Rouhette, *supra* note 5.

[18] The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, *opened for signature* March 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, 847 U.N.T.S. 231 [hereinafter Hague Convention].

[19] *See, e.g.*, Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 530 (1987) (describing the Hague as a system established to make discovery "tolerable" for all states using its procedures); Deman v. Terrien, 2002 WL 1824941 (Cal. Ct. App. 2002) (not officially published) (relying on Hague procedures to avoid the imposition of potential criminal sanctions).

[20] *See* Anglo Am. Ins. Group, P.L.C. v. CalFed Inc., 940 F. Supp. 554 (S.D. N.Y. 1996) (denying request to use Hague Convention procedures noting they are more time consuming than the Federal Rules); Seguros Comercial Americas S.A. De C.V. v. Am. President Lines, Ltd., 933 F. Supp. 1301 (S.D. Tex 1996) (calling the Hague procedures time consuming potentially ineffective); Moake v. Source Int'l Corp., 623 A.2d 263 (N.J. Super. A.D. 1993) (denying the request to use Hague procedures in part because they are more expensive and time consuming than the federal rules).

[21] *See id.* at 542 (calling Hague Convention procedures "unduly time consuming and expensive" and uncertain to produce the desired result).

[22] 482 U.S. 522 (1987).

[23] *See, e.g.*, Sandsend Fin. Consultants, Ltd. v. Wood, 743 S.W.2d 364 (Tex. Ct. App. 1988); Great Lakes Dredge & Dock Co. v. Harnischfeger Corp., 1990 WL 147066 (N.D. Ill. 1990); *In re* Asbestos Litig., 623 A.2d 546 (Del. Super. 1992); *In re* Aircrash Near Roselawn, Ind., 172 F.R.D. 295 (N.D. Ill. 1997); Adm'rs of Tulane Educ. Fund v. Debio Holding S.A., 2000 WL 1131999 (E.D. La. 2000).

[24] *See supra* note 20.

[25] *See* Strauss v. Credit Lyonnais, S.A., 242 F.R.D. 199, 210-223 (E.D.N.Y. 2007) (analyzing each *Aerospatiale* factor separately, but discounting the threat of French criminal sanctions); *In re* Rubber Chem. Antitrust Litig., 486 F.Supp.2d 1078 (N.D.Cal. 2007) (considering the complete comity analysis and finding in favor of non-disclosure); *In re* Payment Interchange Fee & Merch. Disc. Antitrust Litig., 2010 WL 3420517, *7-9 (E.D.N.Y. Aug. 27, 2010) (slip copy) (weighing each Aerospatiale factor and finding foreign interests prohibited disclosure of requested material).

[26] *See generally* Gucci Am., Inc. v. Curveal Fashion, 2010 WL 808639 (S.D.N.Y. Mar. 8, 2010); *In re* Air Cargo Shipping Servs. Antitrust Litig., 2010 WL 1189341 (E.D.N.Y. March 29, 2010).

[27] *Gucci*, 2010 WL 808639 at *8.

[28] *Id.* at *7-8.

[29] *Id.* However, the court left room for protecting the foreign privacy interests implicated if the foreign government indicated intentions to protect its own privacy interests. *Id.* at *8.

[30] *In re Air Cargo*, 2010 WL 1189341 at *3. This court refused to restrict discovery, but recognized the legitimacy of excusing nonproduction when criminal sanctions are realistically possible. *Id.*

[31] *See id.*

[32] Motorola Credit Corp. v. Uzan, 55 Fed. R. Serv. 3d 762 (S.D.N.Y. 2003).

[33] *In re* Daimler Chrysler AG Sec. Litig,, 2003 WL 21698358 (E.D. Mich. 2003)

[34] *See Gucci*, 2010 WL 808639 at *7 (explaining that because defendants provided no evidence of previous enforcement, the court cannot conclude there is a risk of enforcement in the case at hand); *In re Air Cargo*, 2010 WL 1189341 at *2 (explaining that the factual differences between the previous French enforcement of its privacy statute makes it very unlikely the defendant will actually be prosecuted).

[35] *See Uzan*, 2003 WL 203011 (letters from Swiss ambassador); Deman v. Terrien, 2002 WL 1824941 (Cal. App. 2002) (not designated for publication) (refusing to compel defendant to travel to the U.S. for a deposition in part based on the formal protestation letter of a French judicial official).

[36] *See Uzan*, 2003 WL 203011 (considering letters from Swiss ambassador in decision to require Hague procedures for pretrial discovery); Jacobsen v. Deutsche Bank, 206 F. Supp.2d 590, 592 (S.D.N.Y. 2002) (respecting the decision of a German court that journalist privilege prohibited compelling deposition testimony after utilizing Hague procedures [A letter of request]).

[37] *Compare* Ings v. Ferguson, 282 F.2d 149, 151-53 (2d. Cir. 1960) (using letters rogatory to obtain evidence located in foreign jurisdictions) *with* Société Nationale Industrielle Aerospatiale v. United States, 482 U.S. 522 (1987) (holding the Hague Convention is neither the initial nor exclusive remedy for obtaining evidence abroad) *and In re* Vitamins Antitrust Litig., 2001 WL 1029433 (D.D.C. 2001) (holding the Hague Convention procedures were unlikely to result in efficient and timely discovery).

[38] *See* European Commission, Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN (2007), available at http://eur-lex.europa.eu/en /index.htm (last visited October 28, 2010); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047 available at http://eur-lex.europa.

eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML; *see also* Privacy Directive, *supra* note 11, art. 2(a) ("an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or . . . one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.").

[39] *See* Official Journal L 201, 31/07/2002 P. 0037 – 0047, European Commission, Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN (2007), available at http://eur-lex.europa.eu/en/index.htm (last visited October 28, 2010).

[40] FED. R. CIV. P. 34(a) (2007).

[41] *See, e.g.*, *In re* Citric Acid Litig., 191 F.3d 1090, 1107 (9th Cir. 1999) (Explaining that acting as the alter ego or agent of another company can cause a corporation to be deemed to have possession, custody, and control of discovery materials). *Id.*

[42] *See In re* Citric Acid Litig., 191 F.3d at 1107; Cochran Consulting, Inc. v. Uwatec USA, Inc., 102 F.3d 1224, 1229-30 (Fed. Cir. 1996); *In re* Bankers Trust Co., 61 F.3d 465, 469(6th Cir. 1995); Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1426 (7th Cir. 1993); Gerling Int'l Ins. Co. v. Comm'r, 839 F.2d 131, 140-41 (3d Cir. 1988); Searock v. Stripling, 736 F.2d 650, 653 (11th Cir. 1984). Although, entities related more tenuously to one another can also face international discovery complications.

[43] The European Commission and U.S. Department of Commerce have created a framework enabling participants to register and employ the privacy and privacy disclosure protections offered. *See generally*, U.S. Department of Commerce, "Safe Harbor," available at http://www.export.gov/safeharbor/index.html.

[44] It is a violation of some foreign privacy laws for even an entity within that foreign country to collect or review private information, even if it is not transferred outside the country's borders. *See, e.g.*, Article 29 Working Party, WP 55 at p. 21.

[45] *See In re* Citric Acid Litig., 191 F.3d at 1107. The Ninth Circuit Court of Appeals explained that acting as the alter ego or agent of another company can cause a corporation to be deemed to have possession, custody, and control of discovery materials. *Id.*

[46] *See* Privacy Directive, *supra* note 11, art. 8. Article 8 lays out three exceptions to the prohibitions against processing personal information, one of which is obtaining the data subjects consent. *Id.* art. 8(2) (a), 8(2) (b), 8(2) (e).

[47] *See* Working Party, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October* 1995, at 9, 2093/05/EN, WP 114 (Nov. 25, 2005) Article 26(2) (a). To rely on consent it must be specific, informed, and freely given. Specificity requires a particular transfer or series of transfers be consented to and transfers between entities often will not avoid violation through vicarious consent. *Id.*

[48] *See, e.g.*, *In re* Lernout & Hauspie Secs. Litig., 218 F.R.D. 348, 354 (D. Mass. 2003) (acknowledging the redaction of personal information is a valid method of avoiding privacy violations).

[49] Directive 2002/58/EC – Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector as made under Art. 95, Journal Reference L201, 2002-07-31 pp. 37-47, as modified by Directive 2006/24/EC.

[50] *See* FED. R. CIV. P. 34 (1970).

[51] *See, e.g.*, Tracy L. Boyd, *The Information Black Hole: Managing the Issues Arising from the Increase in Electronic Data Discovery in Litigation*, 7 VAND. J. ENT. L. & PRAC. 323 (2005); Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171 (2006); John B. v. Goetz, 531 F.3d 448, 453 (6th Cir. 2008) (describing the involved process of obtaining ESI in the case); Pension Comm. of Univ. of Montreal Pension Plan v. Bank of Am. Secs., LLC, 685 F. Supp.2d 456 (S.D.N.Y. 2010) (listing the extensive electronic materials covered under electronic discovery); Zubulake v. UBS Warburg LLC, 2004 U.S. Dist. LEXIS 13574, at *35 (S.D.N.Y. July 20, 2004) (requiring litigants not only place electronically stored information materials in a litigation hold but also monitor compliance to avoid a potential adverse inference at trial).

[52] *See id.*

[53] *See, e.g.*, *Goetz*, 531 F.3d at 453 (describing the complicated process for obtaining ESI discovery); Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 431 (S.D.N.Y. 2004). Even a cursory review of the case law on e-discovery reveals the significant burden it adds to pretrial preservation and production demands.

[54] *See* FED. R. CIV. P. 37 (2007); *see also Goetz*, 531 F.3d at 453; *Zubulake*, 229 F.R.D. at 431.

Revisiting the Apex Doctrine

By Christopher R. Christensen and Justin M. Schmidt

A FREQUENTLY employed tactic in contentious litigation is the service of a notice seeking the deposition of a senior company executive. Such a tactic is often used for intimidation or harassment of the corporate defendant. The proper response to such a deposition notice is to consider the applicability of the apex doctrine.

As a general matter, the apex doctrine requires the party seeking the deposition of a senior corporate executive to demonstrate that the deponent has relevant – and often unique or superior – knowledge that is unavailable through less intrusive discovery methods. However, the apex doctrine is not an absolute shield for avoiding an apex deposition, particularly if the objections to the deposition merely consist of boilerplate assertions of undue burden, harassment, and the obligatory reminder of the apex deponent's "extremely busy schedule."

Not all jurisdictions recognize the apex doctrine. In such jurisdictions, counsel can often reach the same result by obtaining a protective order to prevent an apex deposition. The specific requirements for obtaining a protective order against an apex deposition vary from jurisdiction to jurisdiction. For instance, some courts place the burden of persuasion on the party seeking to prevent the apex deposition while other courts shift the burden to the party seeking the deposition. Regardless of the jurisdiction, counsel seeking to avoid an apex deposition should file a motion for a protective order that includes an affidavit of the apex deponent detailing the extent of his or her knowledge of and involvement with the dispute, and if applicable, identifying less burdensome methods for obtaining the requested information, such as questioning lower level employees through interrogatories or depositions.

Christopher R. Christensen is a partner with Condon & Forsyth LLP in New York City. He concentrates his practice in the areas of complex aviation, product liability, and commercial litigation.

Justin M. Schmidt is an associate who works in the same practice group

The IADC Privacy Project last addressed the apex doctrine in 2007 with an excellent article by Ralph Streza and Patrick T. Lewis titled *Privacy in the Executive Suite: The Apex Doctrine*, which analyzed the doctrine's origin, application, and leading cases. This is an update to that article. As such, this article focuses on trends and factual nuances in federal and state cases decided since publication of Messrs. Streza and Lewis' article and also identifies federal district courts that have incorporated aspects of the apex doctrine into their local rules.

I. Defining the Apex Doctrine

The apex doctrine is primarily a common law doctrine that allows courts to balance a party's right to liberal discovery with an apex deponent's right to be protected from abuse and harassment.[1] When a party objects to the deposition of an apex deponent (usually by filing a motion for a protective order),

the apex doctrine generally requires courts to consider, before compelling an apex deposition, "whether the executives possess personal or superior [or] unique knowledge" and "whether the information could be obtained from lower level employees or through less burdensome means, such as interrogatories."[2]

Strictly speaking, the apex doctrine requires courts to shift the burden of persuasion of these considerations onto the party seeking the deposition.[3] However, many courts that follow the traditional protective order rule of placing the burden on the party opposing the deposition recognize that apex deponents are particularly susceptible to harassment and abuse and will not hesitate to issue a protective order if warranted under the circumstances.[4] This can be true even of those courts that expressly reject the apex doctrine.[5] In other words, whether a court places the burden of persuasion on the moving or opposing party is not necessarily determinative of whether the court will grant or deny a protective order for an apex deponent.

For procedural purposes, however, it is important to note that courts are split on whether the burden of persuasion lies with the party seeking the deposition[6] or with the party seeking to prevent the deposition.[7] In some states, such as Texas, the state courts place the burden on the former,[8] while the federal courts place the burden on the latter.[9] One Texas federal district court explained that although federal courts apply state substantive law in diversity jurisdiction claims, federal procedural law governs discovery procedures in federal court (i.e., the protective order requirements of Federal Rule of Procedure 26 or the requirements to quash a subpoena under Rule 45(c)).[10] While Rule 26 does require the moving party to show "good cause" for a protective order, many federal courts require the party seeking the deposition to show that the apex deponent has personal or unique knowledge of the dispute or that other discovery methods are unavailable or have been exhausted.[11] To the extent possible, counsel should determine which side of the burden divide the judge in their particular case falls on as judges within the same court may disagree on which party bears the burden.[12]

Regardless of which party the court places the burden of persuasion on, a party seeking to avoid an apex deposition can often attain the same result under either approach with a well-supported motion for a protective order.

II. Who Qualifies as an Apex Deponent?

As a preliminary matter, courts must decide whether the person seeking to invoke the apex doctrine is sufficiently high-ranking. Courts still point to Lee Iacocca, then Chairman of the Board of Chrysler Corporation, in the leading case of *Mulvey v. Chrysler Corp.*[13] as the epitome of an apex deponent.[14] In *Mulvey*, the court required the plaintiff to propound interrogatories instead of deposing Mr. Iacocca because "he is a singularly unique and important individual who can be easily subjected to unwarranted harassment and abuse. He has a right to be protected, and the courts have a duty to recognize his vulnerability."[15] In recent cases, courts had no trouble declaring the following

individuals apex deponents: UAW President Ron Gettelfinger, Continental Airlines CEO Larry Kellner, Google founders Sergey Brin and Larry Page, and Microsoft CEO Steven Ballmer.[16]

Senior management personnel need not be household names or the highest executive in their corporation or organization to be designated an apex deponent. Courts have found a variety of corporate officers and their equivalents in non-corporate organizations[17] to be sufficiently high-ranking for purposes of the apex doctrine, such as chief legal officers, general counsel, executive vice presidents, directors, university presidents, and the Cardinal of the Catholic Archdiocese of New York.[18] No rule defines a specific cut-off point in the corporate hierarchy between apex and non-apex deponents. However, one district court found persuasive the plaintiff's argument that "a vice president position is hardly the 'apex' of a company."[19] Another district court was not convinced that the defendant insurance company's director of corporate claims, vice president of corporate claims, and senior director for corporate claims were "officials or managers at the highest level or 'apex' of corporate management to which the particular rules of apex depositions would apply."[20]

Courts also apply the apex deponent designation to former or retired executive officers.[21] While retired executives may not be able to argue that a deposition would impede their schedules as it would an employed executive, courts will nonetheless evaluate whether the retired executive has unique knowledge of the issues and whether the party seeking the deposition has sought the information through less intrusive means.[22] If the former executive is not retired, but simply employed elsewhere, courts may compare the duties and responsibilities of the current and prior positions to determine whether the executive is still an apex deponent. For example, the district court in *WebSideStory, Inc. v. NetRatings, Inc.* rejected the defendant corporation's contention that the plaintiff's executive whom defendant sought to depose was not an apex deponent because he was no longer the CEO of plaintiff's corporation, but only serving as a director.[23] The court explained that:

> since [the deponent] is currently the CEO and Chairman of the Board of Directors for another company . . . as well as a member of the Board of Directors for WebSideStory and its former CEO, [the deponent] is an official at the highest level or "apex" of a corporation, and while he may not possess the celebrity status of apex deponents in other cases, the Court finds his responsibilities to current and prior employers to be of similar proportions.[24]

The party seeking to have its officer designated an apex deponent should provide the court with information of the company or organization's size, how many people it employs, how many different offices it has, the amount of its business that is concentrated in the region where the officer is employed, and exactly where the officer ranks in the company or organization's hierarchy.[25] Providing this information to the court is

especially important when the size of the company or organization is not readily known.

III. Apex Deponent's Knowledge of the Dispute Is Usually the Deciding Factor

Even if the court designates an individual as an apex deponent, it still may permit the deposition to proceed. This typically occurs when the court finds that the apex deponent has relevant personal knowledge of or involvement in the dispute.

The first question counsel should ask when deciding how to respond to a deposition notice for an apex officer is: What level of knowledge does the deponent have concerning the dispute? The answer to this question usually drives the court's decision on whether to grant or deny a protective order because the apex doctrine "is normally aimed at high level decision makers who have no particular direct knowledge of the facts pertaining to the particular lawsuit."[26]

The requirement of "no particular direct knowledge of the facts" does not mean that a high-level officer must be completely unaware of the issues in the pending litigation for the apex doctrine to apply. Two recent cases demonstrate that CEOs and other high-level officers are often the "public face" of a corporation. Consequently, the fact that they may make public appearances to address events that are the basis of a pending lawsuit does not necessarily mean they have unique or superior knowledge of the issues involved.

The Texas Court of Appeals applied Texas' well-established apex doctrine[27] and held that Continental Airlines' CEO, Larry Kellner, lacked unique or superior knowledge about the causes of a 2008 Continental accident in which 37 passengers were injured.[28] Plaintiffs argued that Kellner had discoverable information about the cause of the accident based on the following: (1) public statements he made after the accident indicating that he would learn the cause of the accident to prevent future accidents; (2) personal letters he sent to each of the passengers; (3) his interviews of flight crew members following the accident; and (4) his knowledge of Continental's implementation of safety policies.[29] Using Kellner's affidavit, the court found that Kellner lacked unique or superior knowledge because the information he gave at a press conference came from other employees; he did not discuss with the flight crew members what occurred before, during, and after the accident; and he did not receive information about the cause of the accident in executive briefings.[30]

Moreover, the court found that plaintiffs had not demonstrated that less intrusive discovery methods had proven insufficient, despite the fact that plaintiffs had submitted 110 requests for production, 74 interrogatories, and taken 11 depositions.[31] The court observed that plaintiffs had not deposed employees with critical information about the accident, including a Rule 30(b)(6)[32] witness, and emphasized that "[m]erely completing some less-intrusive discovery does not trigger an automatic right to depose an apex official."[33] The court held that plaintiffs had failed to show that Kellner's deposition would lead to the discovery of admissible evidence because

his "subjective intent in making the public statements does not establish anything regarding negligence, proximate cause, or damages."[34]

The Michigan Court of Appeals relied extensively on the *Continental Airlines* decision in holding that the apex doctrine protected Toyota's Chairman and CEO and its President and COO from being deposed in a wrongful death action involving the alleged sudden acceleration of a Toyota Camry.[35] Plaintiffs asserted that both executives had made public appearances to discuss Toyota's safety problems and vehicle recall campaign (which did not include the subject vehicle). The court found that the Toyota executives had general knowledge about alleged Camry unintended acceleration issues, but had no unique or superior knowledge of the vehicle's design, testing, and manufacturing process.[36] The court noted that an apex officer "often has no particularized or specialized knowledge of day-to-day operations or of particular factual scenarios that lead to litigation, and has far-reaching and comprehensive employment duties that require a significant time commitment."[37]

The *Continental Airlines* and *Alberto* decisions show that the highest executives in large corporations are often far removed from the issues and events that give rise to litigation. Therefore, such executives usually lack unique or superior knowledge of specific issues in the litigation, which lower level employees most likely possess.

However, the apex doctrine is not an absolute shield that prevents an apex officer from being deposed under any circumstance.[38] For instance, the smaller the corporation, the more likely the apex officer has particular knowledge of or had a role in the dispute and can therefore be deposed.[39] Also, mid-level managers who are not at senior levels of the company are more likely to have discoverable information.[40] Apex officers who are named as individual defendants tend to be more closely associated with the issues in the litigation.[41] Regardless of the size of the company or of the apex officer's rank, courts often will not accept assertions by defense counsel that an apex deposition will result in abuse, harassment, or unreasonable interruption of the officer's busy schedule if the apex deponent is likely to have discoverable information. The following cases illustrate this point.

The Sixth Circuit reversed a district court's denial of plaintiff employee's request to depose her employer's CEO.[42] The employer argued that the CEO was not personally involved in and lacked personal knowledge of the employment decisions that led plaintiff to file discrimination and retaliation claims.[43] The court observed that while plaintiff did not report directly to the CEO (who was the highest ranking officer at a multi-national corporation with over 10,000 employees), the two worked in the same headquarters building, regularly interacted with each other, and were separated by only one direct supervisor.[44] Accordingly, the court found that the CEO had an active role in the adverse employment decisions at issue, and stated that although the record may not currently support a retaliation claim, "it is more than sufficient to support further discovery."[45] Moreover, the court rejected the CEO's "bald assertions" that the deposition would pose an undue

burden because other executives had already been deposed and the CEO likely had information critical to the plaintiff's claims.[46]

The Western District of Arkansas denied a protective order for Wal-Mart's CEO and its Executive Vice President despite Wal-Mart's contention that the apex doctrine should apply and that the depositions "would cause 'annoyance, embarrassment, oppression, or undue burden and expense.'"[47] The court noted that the test for deciding a motion for a protective order "is not whether a putative deponent had personal involvement in an event, or even whether they have 'direct' knowledge of the event, but whether the witness may have information from whatever source that is relevant to a claim or defense."[48] The court found that the executives may have relevant information about their instructions not to shred documents pertinent to a government investigation and whether their employees followed the instructions.[49]

These cases demonstrate that apex officers of any level can be deposed if the court concludes that they possess relevant, unique, or superior knowledge of issues in the litigation. Even if a court issues a protective order on the grounds that lower level employees have not been deposed or other less intrusive discovery means have not been exhausted, courts will often permit a party to renew its request to depose an apex officer if it shows that the alternate discovery methods proved insufficient.[50]

IV. Limitations on Apex Depositions

Due to the broad discovery rules in state and federal courts, some courts may be disinclined to grant a motion that seeks to completely prevent an apex deposition. For example, one district court in deciding whether to completely prohibit an apex deposition found that:

> [T]he issuance of a broad protective order precluding any discovery from [an apex deponent] goes too far. Given the fact that knowledge is frequently proved circumstantially, precluding all discovery of a highly placed business, government or clerical official based solely on their unchallenged denial of knowledge sets the bar for a protective order too low. . . . [P]arties to an action are ordinarily entitled to test a claim by a potential witness that he has no knowledge.[51]

Depending on the court's prior disposition to such prophylactic motions, counsel may want to consider requesting certain limitations on taking the apex deposition, rather than (or in the alternative to) requesting complete prevention of the deposition. Counsel may be able to avoid or at least defer an oral deposition by proposing that the apex deponent answer interrogatory questions or written deposition questions.[52] Courts also may allow depositions to be conducted by telephone or video conference.[53]

Standard oral depositions, however, may not always be avoidable. Fortunately, courts have granted a wide range of limitations on oral apex depositions. One of the most commonly granted limitations relates to the deposition location. The general rule is that depositions of apex deponents "'are

ordinarily taken at the [deponent's] principal place of business unless justice requires otherwise.'"[54] Courts often grant time restrictions on oral apex depositions, limiting the deposition to less than the seven hours allotted under Federal Rule of Civil Procedure 30(d)(1).[55] Counsel may also request that the scope of inquiry be narrowed to specific issues in the case.[56]

Courts may take into consideration the health and age of the apex deponent. The standard for "'seeking to prevent or delay a deposition by reason of medical grounds'" is that "'the moving party has the burden of making a *specific and documented factual showing* that the deposition would be dangerous to the deponent's health.'"[57] Brief and conclusory doctor's notes are insufficient.[58] Even without a documented medical condition, however, a court may limit an apex deposition based on the deponent's age. In *Minter v. Wells Fargo Bank, N.A.*, the court limited the 75-year old deponent's deposition to five hours on the first day and two hours on the second day, even though he submitted no opinion from a medical professional and merely asserted that "he has health problems that 'flare up from time to time' and his 'stamina has declined over the years.'"[59]

Finally, parties may enter into discovery agreements with opposing counsel that provide restrictions or logistical conditions for taking apex depositions. In a case involving the explosion of a BP oil refinery in Texas City, Texas, that killed fifteen people, the Texas Supreme Court directed a trial court to enforce the parties' discovery agreement, which limited BP's CEO's deposition to one hour by telephone.[60]

V. Incorporation of the Apex Doctrine into Local Rules

Several federal district courts have incorporated aspects of the apex doctrine into their local rules.[61]

The Eastern District of New York Local Rule 30.5 provides:

> (a) Where an officer, director or managing agent of a corporation or a government official is served with a notice of deposition or subpoena regarding a matter about which he or she has no knowledge, he or she may submit reasonably before the date noticed for the deposition an affidavit to the noticing party so stating and identifying a person within the corporation or government entity having knowledge of the subject matter involved in the pending action.
>
> (b) The noticing party may, notwithstanding such affidavit of the noticed witness, proceed with the deposition, subject to the witness's right to seek a protective order.

Rule 30.5 allows a corporate or government officer noticed for a deposition to designate a Rule 30(b)(6) witness to testify on behalf of the corporation or government body regarding the issues involved in the litigation. The noticing party may accept

the Rule 30(b)(6) witness or proceed with the apex deposition subject to the deponent's right to file a motion for a protective order.

The language of District of Wyoming Local Rule 30.1 is nearly identical to that of Eastern District of New York Local Rule 30.5. The District of Kansas provides a document titled "Deposition Guidelines," which is separate from its local rules, but contains a paragraph titled "Depositions of Witnesses Who Have No Knowledge of the Facts," which also is nearly identical to the local rules mentioned above.[62]

The Eastern District of Virginia's Local Rule 45 requires permission of the court before issuing a subpoena for the attendance at any hearing, trial, or deposition of the following government officials:

> (1) the Governor, Lieutenant Governor, or Attorney General of any State; (2) a judge of any court; (3) the President or Vice-President of the United States; (3) any member of the President's Cabinet; (5) any Ambassador or Consul; or (6) any military officer holding the rank of Admiral or General.

In addition to local rules, some district court judges have incorporated aspects of the apex doctrine into their case management orders and pretrial orders.[63]

VI. Conclusion

The apex doctrine provides counsel with the ability to avoid, or at least limit, the deposition of a high-ranking executive or officer. Before filing a motion for a protective order to prevent an apex deposition, counsel should thoroughly familiarize themselves with the apex doctrine's procedural and substantive nuances, which vary depending on the jurisdiction or judge, such as which party has the burden of persuasion, who qualifies as an apex officer, and what factual information the court requires to apply the doctrine. Counsel also should determine whether the local rules incorporate elements of the apex doctrine or consider requesting that the court place any guidelines pertaining to apex depositions in the case management, pretrial, or scheduling orders.

Even in those courts that reject or do not expressly apply the apex doctrine, the party seeking to avoid an apex deposition can often obtain the same relief with a well-supported motion for a protective order. No apex deponent is immune from being deposed, especially if the officer has relevant, unique, or superior knowledge of the issues in the case that cannot be obtained through alternative discovery methods. Under these circumstances, counsel should seek to achieve reasonable limitations on the time, place, scope, and/or method of the deposition.

---

[1] *See* Abarca v. Merck & Co., No. 07 Civ. 0388, 2009 WL 2390583, at *3 (E.D. Cal. Aug. 3, 2009) ("'Virtually every court that has addressed deposition notices directed at an official at the highest level or 'apex' of corporate management has observed that such discovery creates a tremendous potential for abuse or harassment.'" (citations omitted)).

[2] Reif v. CNA, 248 F.R.D. 448, 451 (E.D. Pa. 2008) (analyzing a number of leading apex doctrine cases).

[3] *See* Crest Infiniti II, LP v. Swinton, 174 P.3d 996, 1003 (Okla. 2007) (citing Crown Cent. Petroleum Corp. v. Garcia, 904 S.W.2d 125, 128 (Tex. 1995)); *see also* Gauthier v. Union Pac. R.R. Co., No. 07 Civ. 12, 2008 WL 2467016, at *4 n.2 (E.D. Tex. June 18, 2008); Alberto v. Toyota Motor Corp., No. 296824, 2010 WL 3057755, slip op. at 3 (Mich. Ct. App. Aug. 5, 2010) (the page numbers cited for this case refer to the court's slip opinion because the Westlaw version was not paginated when this article went to print).

[4] *See, e.g.*, Tabor v. Hilti, Inc., No. 09 Civ. 189, 2010 WL 2990004, at *1 (N.D. Okla. July 23, 2010); Mehmet v. PayPal, Inc., No. 08 Civ. 1961, 2009 WL 921637, at *3 (N.D. Cal. Apr. 3, 2009); Stelor Prods., Inc. v. Google, Inc., No. 05 Civ. 80387, 2008 WL 4218107, at *5 (S.D. Fla. Sept. 15, 2008); Bouchard v. N.Y. Archdiocese, No. 04 Civ. 9978, 2007 WL 2728666, at *6 (S.D.N.Y. Sept. 19, 2007), *aff'd*, 2007 WL 4563492 (S.D.N.Y. Dec. 18, 2007).

[5] *See, e.g.*, *Gauthier*, 2008 WL 2467016, at *4 & n.2 (rejecting the "Texas apex doctrine," which shifts the burden to plaintiffs, yet quashing executives' depositions and requiring plaintiffs to "first attempt to obtain the sought information through the less burdensome means of discovery described herein").

[6] *See, e.g.*, *Abarca*, 2009 WL 2390583, at *4; Chick-Fil-A, Inc. v. CFT Dev., LLC, No. 07 Civ. 501, 2009 WL 928226, at *1 (M.D. Fla. Apr. 3, 2009); Wagner v. Novartis Pharm. Corp., No. 07 Civ. 129, 2007 WL 3341845, at *1 (E.D. Tenn. Nov. 8, 2007); *Alberto*, 2010 WL 3057755, slip op. at 3.

[7] *See, e.g.*, Meharg v. I-Flow Corp., No. 08 Civ. 0184, 2009 WL 1404603, at *1 (S.D. Ind. May 15, 2009) (citing *In re* Bridgestone/Firestone Inc. Tires Prods. Liab. Litig., 205 F.R.D. 535, 536 (S.D. Ind. 2002) (determining that decisions where courts imposed a burden on the proponent to demonstrate unique personal knowledge by an executive before being deposed does not establish "rigid adherence to the burdens imposed under the facts of those cases")); Prosonic Corp. v. Stafford, No. 07 Civ. 803, 2008 WL 64710, at *1 (S.D. Ohio Jan. 3, 2008); *Bouchard*, 2007 WL 2728666, at *4.

[8] *See In re* Cont'l Airlines, Inc., 305 S.W.3d 849, 852 (Tex. App. 2010).

[9] *See* Staton Holdings, Inc. v. Russell Athletic, Inc., No. 09 Civ. 0419, 2010 WL 1372479, at *2-3 (N.D. Tex. Apr. 7, 2010); *Gauthier*, 2008 WL 2467016, at *3.

[10] *See Gauthier*, 2008 WL 2467016, at *4 n.2 (finding "no federal cases within the Fifth Circuit actually applying the Texas standard for the apex doctrine").

[11] *See* federal cases cited *supra* note 6.

[12] *Compare* Mansourian v. Bd. of Regents of Univ. of Cal. at Davis, No. 03 Civ. 2591, 2007 WL 4557104, at *3 & n.2 (E.D. Cal. Nov. 21, 2007) (deciding not to apply the apex doctrine burden-shifting approach because no Ninth Circuit or Supreme Court precedent requires that result, however, noting that the burden-shifting approach could be applied under certain circumstances) *with* Abarca v. Merck & Co., No. 07 Civ. 0388, 2009 WL 2390583, at *4 (E.D. Cal. Aug. 3, 2009) (finding that "the burden-shifting approach provides guidance to this Court").

[13] 106 F.R.D. 364 (D.R.I. 1985).

[14] *See, e.g.*, Berning v. UAW Local 2209, 242 F.R.D. 510, 513-14 (N.D. Ind. 2007); Wal-Mart Stores, Inc. v. Vidalakis, No. 07-MC-00039, 2007 WL 4591569, at *2 (W.D. Ark. Dec. 28, 2007).

[15] *Mulvey*, 106 F.R.D. at 366.

[16] *See Berning*, 242 F.R.D. at 513-14 ("Gettelfinger, in his position as the President of the International UAW [overseeing more than 600 staff members in a union with over 1.3 million members], is particularly vulnerable to unwarranted harassment and abuse that [plaintiff's] deposition may produce, and he has a right to be protected from such harassment."); *Cont'l Airlines*, 305

S.W.3d at 859; Stelor Prods., Inc. v. Google, Inc., No. 05 Civ. 80387, 2008 WL 4218107, at *4-5 (S.D. Fla. Sept. 15, 2008) (Google founders); Kelley v. Microsoft Corp., No. C07-0475, 2008 WL 5000278, at *1-2 (W.D. Wash. Nov. 21, 2008) (recognizing Microsoft's CEO as an apex deponent, yet denying his motion for protective order).

[17] Courts often bar the depositions of high-ranking government officials under the *Morgan* doctrine, a doctrine similar to the apex doctrine. *See, e.g.*, United States v. Sensient Colors, Inc., 649 F. Supp.2d 309, 316-18 (D.N.J. 2009) (applying the *Morgan* doctrine to bar the deposition of a former Administrator of the EPA).

[18] *See* Dart Indus., Inc. v. Acor, No. 06 Civ. 1864, 2008 WL 1995105, at *1 (M.D. Fla. May 7, 2008) ("no question" that the Secretary, Chief Legal Officer and Executive Vice-President of Tupperware was a "high-ranking executive officer"); Burns v. Bank of Am., No. 03 Civ. 1685, 2007 WL 1589437, at *3 (S.D.N.Y. June 4, 2007) (general counsel); Parmer v. Wells Fargo & Co., No. 07 Civ. 02061, 2009 WL 1392081, at *1-4 (D. Colo. May 15, 2009) (executive vice president); Roman v. Cumberland Ins. Group, No. 07 Civ. 1201, 2007 WL 4893479, at *1 (E.D. Pa. Oct. 26, 2007) (company president, vice president, and board of directors); Raml v. Creighton Univ., No. 08 Civ. 419, 2009 WL 3335929, at *1-3 (D. Neb. Oct. 15, 2009) (Creighton University President); Mansourian v. Bd. of Regents of Univ. of Cal. at Davis, No. 03 Civ. 2591, 2007 WL 4557104, at *1-2 & n.2 (E.D. Cal. Nov. 21, 2007) (Chancellor of the University of California at Davis); Bouchard v. N.Y. Archdiocese, No. 04 Civ. 9978, 2007 WL 2728666, at *3-4 (S.D.N.Y. Sept. 19, 2007) (relying on cases involving corporate executives to partially grant a protective order for Cardinal Egan), *aff'd*, 2007 WL 4563492 (S.D.N.Y. Dec. 18, 2007).

[19] Kelly v. Provident Life & Accident Ins. Co., 695 F. Supp.2d 149, 157 (D. Vt. 2010) (denying insurance company's motion for a protective order for its regional vice president of claims).

[20] Lexington Ins. Co. v. Sentry Select Ins. Co., No. 08 Civ. 1539, 2009 WL 4885173, at *7 (E.D. Cal. Dec. 17, 2009).

[21] Rodriguez v. SLM Corp., No. 07 Civ. 1866, 2010 WL 1286989, at *1-3 (D. Conn. Mar. 26, 2010) ("The standards that govern depositions of corporate executives apply with equal force to former executives.").

[22] *Id.*

[23] No. 06 Civ. 408, 2007 WL 1120567, at *3 (S.D. Cal. Apr. 6, 2007).

[24] *Id.*

[25] *See* Prosonic Corp. v. Stafford, No. 07 Civ. 803, 2008 WL 64710, at *1-2 (S.D. Ohio Jan. 3, 2008) (due to defendant's lack of factual detail, the court was unable to determine whether the district manager was sufficiently high-ranking to be "subject to more exacting scrutiny by the Court than a garden-variety request to take a deposition").

[26] Wal-Mart Stores, Inc. v. Vidalakis, No. 07-MC-00039, 2007 WL 4591569, at *1 (W.D. Ark. Dec. 28, 2007); *see also* Abarca v. Merck & Co., No. 07 Civ. 0388, 2009 WL 2390583, at *5 (E.D. Cal. Aug. 3, 2009) (granting protective order because "there is no indication that [Merck's CEO] has unique, non-cumulative knowledge simply because his name appears on three documents, particularly where one is an unsigned draft, one is not addressed to or from him and another is an apparently unrelated e-mail string addressed to [him] and other individuals"); Alliance Indus., Inc. v. Longyear Holdings, Inc., No. 08 Civ. 490S, 2010 WL 4323071, at *4 (W.D.N.Y. Mar. 19, 2010) (granting protective order for CEO and explaining that "'Apex' depositions are disfavored in th[e Second] Circuit 'unless [the executives] have personal knowledge of relevant facts or some unique knowledge that is relevant to the action'" (citation omitted)).

[27] *See In re* BP Prod. N. Am., Inc., 244 S.W.3d 840, 842 n.2 (Tex. 2008).

[28] *See In re* Cont'l Airlines, Inc., 305 S.W.3d 849, 858 (Tex. App. 2010).
[29] *Id.* at 851.
[30] *Id.* at 858.
[31] *Id.* at 858-59.
[32] A Rule 30(b)(6) witness is chosen by a company to testify on behalf of the company, rather than in the witness's individual capacity.
[33] *See Cont'l Airlines*, 305 S.W.3d at 858-59.
[34] *Id.* at 859.
[35] Alberto v. Toyota Motor Corp., No. 296824, 2010 WL 3057755, slip op. at 8 (Mich. Ct. App. Aug. 5, 2010).
[36] *Id.*
[37] *Id.* at 6.
[38] *Id.* at 5; *see also* Echostar Satellite, LLC v. Splash Media Partners, L.P., No. 07 Civ. 02611, 2009 WL 1328226, at *2 (D. Colo. May 11, 2009) (noting that "'highly-placed executives are not immune from discovery'" (citation omitted)); Otsuka Pharm. Co. v. Apotex Corp., No. 07 Civ. 1000, 2008 WL 4424812, at *5 (D.N.J. Sept. 25, 2008) ("[M]ultiple jurisdictions recognize that there is not a protective blanket that prohibits discovery from highly-placed executives.").
[39] *See, e.g.*, Ray v. BlueHippo, No. 06 Civ. 1807, 2008 WL 4830747, at *2 (N.D. Cal. Nov. 6, 2008) (finding that the CEO had "personal knowledge, which is not surprising given that BlueHippo is a relatively small company, not a large national corporation").
[40] *See, e.g.*, Wal-Mart Stores, Inc. v. Vidalakis, No. 07-MC-00039, 2007 WL 4591569, at *1-2 (W.D. Ark. Dec. 28, 2007) (distinguishing Wal-Mart real estate managers from top-level apex officers and finding that the managers may have unique and necessary information concerning the real estate contracts at issue).
[41] *See, e.g.*, Anthropologie, Inc. v. Forever 21, Inc., No. 07 Civ. 7873, 2009 WL 723158, at *1 (S.D.N.Y. Mar. 11, 2009); *Ray*, 2008 WL 4830747, at *1.
[42] *See* Conti v. Am. Axle & Mfg., 326 F. App'x 900, 901-02 (6th Cir. 2009).
[43] *Id.* at 904.
[44] *Id.* at 906.
[45] *Id.* at 905-06.
[46] *Id.* at 907.
[47] Mills v. Wal-Mart Stores, Inc., No. 06 Civ. 5162, 2007 WL 2298249, at *1 (W.D. Ark. Aug. 7, 2007).
[48] *Id.* at *2; *see also* Johnson v. Jung, 242 F.R.D. 481, 483 (N.D. Ill. 2007) (denying protective order for CEO despite her claims that she lacked personal involvement because she likely had relevant knowledge of issues in the case).
[49] *Mills*, 2007 WL 2298249, at *2.
[50] *See, e.g.*, Gauthier v. Union Pac. R.R. Co., No. 07 Civ. 12, 2008 WL 2467016, at *4 (E.D. Tex. June 18, 2008) (quashing the depositions of the Union Pacific executives, but warning that the deposition requests may be revisited if plaintiffs show they were unable to obtain the necessary information through less burdensome means of discovery); *see also* Mehmet v. PayPal, Inc., No. 08 Civ. 1961, 2009 WL 921637, at *3 (N.D. Cal. Apr. 3, 2009); Reif v. CNA, 248 F.R.D. 448, 455 (E.D. Pa. 2008).
[51] Bouchard v. N.Y. Archdiocese, No. 04 Civ. 9978, 2007 WL 2728666, at *4 (S.D.N.Y. Sept. 19, 2007), *aff'd*, 2007 WL 4563492 (S.D.N.Y. Dec. 18, 2007).
[52] *See, e.g.*, Elvig v. Nintendo of Am., Inc., No. 08 Civ. 02616, 2009 WL 2399930, at *3 (D. Colo. July 31, 2009) (interrogatories or written deposition questions under Federal Rule of Civil Procedure 31); Craig & Landreth, Inc. v. Mazda Motor of Am., Inc., No. 07 Civ. 134, 2009 WL 103650, at *2 (S.D. Ind. Jan. 12, 2009) (interrogatories); *Bouchard*, 2007 WL 2728666, at *5 (permitting plaintiff to serve 25 deposition questions in lieu of an oral deposition).
[53] Alexander v. Johns Manville, Inc., No. 09 Civ. 0518, 2010 WL 597984, at *1 (S.D. Ind. Feb. 17, 2010) (providing the option to depose manager by telephone); Kirk v. Shaw Envtl., Inc., No. 09 Civ. 1405, 2010 WL 447264, at

*4 n.3 (N.D. Ohio Feb. 3, 2010) (video conferencing possible, presumably if both parties agree); *In re* Jarvar, Nos. 04-62762-7 & 09-00028, 2009 WL 5247491, at *4 n.5 (Bankr. D. Mont. Dec. 28, 2009) (video conferencing permitted if both parties agree).

[54] Crest Infiniti II, LP v. Swinton, 174 P.3d 996, 1003 n.16 (Okla. 2007).

[55] *See, e.g.*, Mformation Techs., Inc. v. Research In Motion, Ltd., No. 08 Civ. 04990, 2010 WL 3154355, at *2 (N.D. Cal. Aug. 9, 2010) (1 hour); *Kirk*, 2010 WL 447264, at *4 (90 minutes); Raml v. Creighton Univ., No. 08 Civ. 419, 2009 WL 3335929, at *3 (D. Neb. Oct. 15, 2009) (2 hours); DR Sys., Inc. v. Eastman Kodak Co., No. 08 Civ. 669, 2009 WL 2973008, at *7 (S.D. Cal. Sept. 14, 2009) (3 hours); Kelley v. Microsoft Corp., No. C07-0475, 2008 WL 5000278, at *2 (W.D. Wash. Nov. 21, 2008) (3 hours); *In re* Land, No. 100796/08, 2009 WL 241728, at *5 (N.Y. Sup. Ct. N.Y. County Jan. 6, 2009) (2 hours).

[56] *See, e.g.*, *Raml*, 2009 WL 3335929, at *3; Meharg v. I-Flow Corp., No. 08 Civ. 0184, 2009 WL 1404603, at *3 (S.D. Ind. May 15, 2009); *Kelley*, 2008 WL 5000278, at *2; *In re* Land, 2009 WL 241728, at *5.

[57] Minter v. Wells Fargo Bank, N.A., 258 F.R.D. 118, 127 (D. Md. 2009) (citation omitted) (emphasis added by the *Minter* court).

[58] *Id.* at 127-28.

[59] *Id.* at 128.

[60] *See In re* BP Prod. N. Am., Inc., 244 S.W.3d 840, 848 (Tex. 2008).

[61] Due to the sheer number of state, county, and local courts, only the local rules for federal courts were reviewed.

[62] Deposition Guidelines, *available at* http: //www.ksd.uscourts.gov/guidelines/depo guidelines.pdf.

[63] *See, e.g.*, *In re* Seroquel Prods. Liab. Litig., No. 6:06-md-1769 (M.D. Fla.), Case Management Order No. 3, filed Apr. 13, 2007; *In re* Propulsid Prods. Liab. Litig., MDL No. 1355 (E.D. La.), Pretrial Order No. 7, filed Dec. 7, 2000. The language in both of these orders is practically identical to the language in the above-mentioned local rules for the Eastern District of New York., District of Wyoming, and the District of Kansas's Deposition Guidelines.