

Keeping Up with the Millennials—The Use and Ramifications of Technology

Lew R.C. Bricker

SmithAmundsen LLC

150 N. Michigan Ave., Ste. 3300

Chicago, IL 60601

(312) 894-3200

(312) 894-3210 [fax]

lbricker@salawus.com

James A. Mullen

Werner Enterprises

14507 Frontier Road

Omaha, NE 68138

(402) 895-6640

jmullen@werner.com

[Return to course materials table of contents](#)

LEW BRICKER is a partner with SmithAmundsen LLC in Chicago, Illinois where he chairs the Commercial Transportation and E- Discovery Groups and leads its Rapid Response Team. He represents motor carriers, logistics providers, product manufacturers and their insurers in both state and federal court. He speaks and writes regularly on issues affecting the commercial transportation industry and the effects of technology on litigation. He has been named an Illinois *Super Lawyer* since 2007 in transportation law by *Law & Politics* magazine and he serves as a contributing author to the Chicago Traffic Club. Mr. Bricker is a member of DRI, TIDA, TLA, the Chicago Traffic Club and the IWLA.

JIM MULLEN is Vice President and General Counsel of Litigation of Werner Enterprises, Inc. Werner is a transportation and freight management company that is headquartered in Omaha, Nebraska, and does business in the US, Canada, Mexico, China and Australia. Mr. Mullen was in an active trial practice from 1993 - 2006, and is a member of the American Board of Trial Advocates. He is responsible for the Litigation, Risk and Safety Departments at Werner.

Keeping Up with the Millennials—The Use and Ramifications of Technology

Table of Contents

I. Introduction.....	169
II. Where to Look	169
A. Types of Information Available.....	170
III. The Ethics of the Web Based Investigation and Search.....	171
IV. Where to Look—Issuing Discovery	173
A. Interrogatories	173
V. Discovery and Admissibility	175
A. Publicly Displayed Information Has No Expectation of Privacy	175
B. Court Cases Addressing Possible Uses of Web Based Information.....	177
C. Effects of the Stored Communications Act (SCA) on Discoverability of Electronically Communicated Information.....	178
VI. Jury Duty.....	181
VII. Service of Process	181
VIII. Texting, Social Networking and the Commercial Transportation Industry.....	182
IX. Google Scholar	182
X. Conclusion	183
Appendix A	184
Appendix B.....	191

Keeping Up with the Millennials—The Use and Ramifications of Technology

I. Introduction

Technology is a part of our everyday lives; we cannot avoid it, even if we want to. In litigation, traditional discovery means the exchange of paper and lots of it. With the not so new world order, you ignore technology and what it has to offer—both positive and adverse—at your peril. In this paper we examine some of the common methods for accessing electronically stored information and the pitfalls associated with acquiring and using it in litigation.

Website providers, the courts and opposing counsel protect and limit the data that can be accessed and discovered. Whether it is Facebook, Google or some other website, those responsible for maintaining the sites have often enacted stringent policies that limit access by third parties and non-members to them. Sometimes you will get lucky and find what you need with a few simple clicks, but more often than not, that is not the case. Acquiring useful information is more complicated than simply typing in what you are looking for into Google or serving a subpoena. Parties aggressively work to limit what is disclosed once they realize that what they have, or in some cases, might have, posted on the Web is now in play. Further, courts have treated the discovery of electronically stored information more stringently since the enactment of the Amended Federal Rules of Civil Procedure in December of 2006. The trend in the courts appears to be requiring parties to limit and tailor their discovery requests and responses. Courts no longer accept broad requests that are not narrowly tailored and targeted. Similarly, courts no longer permit the dumping of data in an effort to bury a case in discovery. In concluding his feelings about a discovery dispute, Federal Magistrate Judge Maas observed that one particular case had become “bogged down in expensive and time-consuming litigation of electronic discovery issues only tangentially related to the underlying merits of the plaintiffs’ . . . claims.” *Aguilar v. Immigration and Customs Enforcement Div.*, 255 F.R.D. 350, 364 (S.D.N.Y. 2008).

For some reason, people often treat their technologically based activities differently from how they act with more traditional means. In other words, people will write and send an email or post on a website words, photos and thoughts that they would never put in a traditional letter or utter on the telephone. It is akin to the surveillance video of a plaintiff engaging in activities that she has said she could no longer perform. Perhaps, the computer monitor or impersonal nature of the electronic transaction provides the individual with anonymity or strength that allows her to be more courageous or, it would seem, not so bright. These internet based activities can yield a treasure trove of information for the searcher willing to invest the time, persistence and effort to look. These items can include photos, descriptions of activities, search histories, friends, business contacts and even personal discussions. In 2001, Chris Sherman and Gary Price wrote a book entitled *The Invisible Web—Uncovering Information Sources Search Engines Can’t See*. The premise of their thesis was that a host of information exists that traditional search engines such as Google and Yahoo cannot and do not retrieve. Chris Sherman and Gary Price, *The Invisible Web—Uncovering Information Sources Search Engines Can’t See*, Information Today, Inc., Medford, NJ, 2001, at p. 2. Since 2001, improvements in technology coupled with the explosion of available data have made searching the Web easier and more fruitful for the enterprising sleuth.

II. Where to Look

There is what can only be described as an immeasurable amount of data that can be searched. This makes the search both potentially frustrating and profitable. In December of 2008, Netcraft estimated that

there were almost 187 million websites. http://news.netcraft.com/archives/2008/12/24/december_2008_web_server_survey.html. In October of that same year, Facebook estimated that it hosted its 10 billionth photo. http://www.facebook.com/note.php?note_id=30695603919. In June of 2009, Facebook stated that on average at least one billion messages a day flowed through its site. <http://www.facebook.com/notes.php?id=9445547199&start=10&hash=4d57f885e71f330a971dd56dae6b7f99>. Currently, there are more than 300 million Facebook users worldwide with approximately 70 million of them based in the United States. <http://www.facebook.com/press/info.php?statistics>. The company's fastest growing demographic is individuals 35 years and older. <http://www.web-strategist.com/blog/2009/01/11/a-collection-of-soical-network-stats-for-2009/>. For comparison purposes, MySpace has a similar number of users as Facebook, but they are generally younger. *Id.* Meanwhile, in July of 2009, the Radicati Group estimated that 247 billion email messages were sent per day on average in 2009 and that the number would almost double by 2013. <http://www.radicati.com/?p=3237>. The key becomes locating and finding the data in a usable, relevant and admissible manner.

A. Types of Information Available

Various types of information exist on websites—restricted and unrestricted. The data can include public and private information, information that can be only acquired via subpoena and archival information.

Anyone can look at unrestricted information. Most, if not all, sites that allow the input of data, however, permit the user to select privacy settings that limit what the general public can view. The private information typically requires registration, a password and/or some form of a login or username to gain access to it. Those searching for data must be aware of their ethical and legal obligations when engaging in internet based searches, which are addressed further below. Nonetheless, the public information can often include photos, descriptions, identification of friends and other information that can prove useful to the litigant.

Social networking sites are often the best and most profitable sites to search when looking for information on an individual. They can include contact information, education and employment histories, photos, videos, emails, messages, lists of friends, associate information and other personal data. This data can and is being used by companies all over the world to challenge the veracity of claims that are being made. For example, a Canadian woman had her medical benefits cancelled after her health care insurers found her engaging in activities contrary to their view of the diagnosis of major depression that she had been given by her physicians. <http://abcnews.go.com/International/wireStory?id=9147300>.

Almost 56 million adults in the United States now visit social networks at least monthly, according to Forrester Research. <http://mashable.com/2009/07/28/social-networking-users-us/>. The most prevalent social networking websites are Facebook and MySpace. Limiting a search to these two, however, would result in an incomplete undertaking. Others identified in one list of the top ten most popular social networking sites include: Twitter, Fixster, LinkedIn, Tagged, Classmates, MyYearbook, LiveJournal and Imeem. <http://social-media-optimization.com/2009/02/top-twenty-five-social-networking-sites-feb-2009/>. Of note, Twitter advises its members/users that once a person Tweets, the posting is available to the world. <https://twitter.com/tos>. Other growing sites include those used for internet dating, such as EHarmony, Match.com, Yahoo! Personals, Chemistry.com, PerfectDate.com and JDate. These sites have more than 60 million users between them. <http://www.consumer-rankings.com/Dating/?c=4&e=r&ch=1&ad=3773827780&sc=search&kw=online percent20ating&ag=1339548640&cr=14362201&gclid=CN0do-2Irp4CFUlo5QodWw1lmw>.

When using social network sites to investigate individuals, it is important to also recognize that like society, the sites can have distinct membership profiles. For example, a recent story on National Public Radio pointed out that the groups utilizing these websites are being targeted and even divided on cultural grounds. Laura Sydell, *Facebook, MySpace Divide Along Social Lines*, National Public Radio, October 21, 2009 at <http://>

www.npr.org/templates/story/story.php?storyId=113974893. MySpace has a Hispanic oriented version called MySpace España, while Facebook started out as a tool for college students to keep in touch. Now, NPR suggests that more diverse groups turn to MySpace as their social network portal of choice. This type of information can be an important piece of knowledge when pursuing information about a person and searching the Web.

The website Spokeo allows users to search multiple social networking sites at a time with the aid of a single email address to see if individuals are listed. http://www.spokeo.com/blog/?page_id=2. Results can include photos, business information, social networking information, email confirmation and domain information. Another site, Intelius, offers people, background commercial and a host of other searches. <http://www.intelius.com/>. Though casting a broader and more targeted reach, Spokeo and Intelius are not all inclusive. They simply could never be.

Archived websites also contain information that has been replaced or superseded by newer data. Like libraries collect books and magazines of long ago, so do certain websites. One site that can prove helpful when researching companies or individuals and what they used to post online is Archive.org. Archive.org “is a 501(c)(3) non-profit that was founded to build an Internet library. Its purposes include offering permanent access for researchers, historians, scholars, people with disabilities, and the general public to historical collections that exist in digital format.” <http://www.archive.org/about/about.php>. An example of the type of information that might be found is an old version of a company website and the representations made on it.

Though much data can be accessed without a subpoena, often they are required. The following section on discovery and Appendix A offer some insights into and suggestions for acquiring protected or restricted data. Websites differ in how closely they guard and release information.

III. The Ethics of the Web Based Investigation and Search

One of the most popular aspects of the Internet is that it permits anonymity. Usernames, the modern day version of the *nom de guerre*, allow an individual to voice an opinion without identifying who he may be. In the same vein, this impersonal persona permits a stranger to make contact with a person without open and complete disclosure about who he might be and any agenda he might be pursuing. This anonymity might tempt the investigator to make contact with an opposing party or claimant via shadowy and improper means.

Both the federal and state governments have attempted to regulate the access of information on the Internet. The Stored Wire and Electronic Communications and Transactional Records Access Act more commonly known as the Stored Communications Act (“SCA”), 18 U.S.C.S. §§2701-2711, prevents providers of communication services from divulging private communications to certain entities and/or individuals. The SCA was enacted because the Internet presented numerous potential privacy breaches that the Fourth Amendment does not specifically address. The SCA governs liability for both electronic communication service (ECS) and remote computing service (RCS) providers. An ECS is any service which provides to its users the ability to send or receive wire or electronic communications. An RCS is a service that provides to the public computer storage or processing services by means of an electronic communications system. Both an ECS and RCS can release private information to, or with the lawful consent of, *an addressee or intended recipient* of such communication. On the other hand, only an RCS can release private information with the lawful consent of *the subscriber*. See *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900-01 (9th Cir. 2008).

States have not acted as pervasively as the federal government. Some states, however, do maintain laws limiting the disclosure of privacy information by Internet Service Providers, of employee email and internet activity and of what the operators of websites may disclose. See <http://www.ncsl.org/default.aspx?tabid=13463#buspolicies>.

Information kept in plain view is not subject to ethical restriction in its viewing or use. In *Moreno v. Hanford Sentinel, Inc.*, the court explained why searching a public space such as a public page on a website is not improper. *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 91 Cal. Rptr. 3d 858 (Cal. Ct. App. 2009). “[A] crucial ingredient of the applicable invasion of privacy cause of action is a public disclosure of *private facts*. A matter that is already public or that has previously become part of the public domain is not private.” *Id.* at 1130; see also, *State ex rel. State Farm Fire & Casualty Co. v. Madden*, 192 W. Va. 155, 451 S.E.2d 721, 730 (W. Va. 1994) (noting that activities that “occurred in full view of the general public” need not be excluded as improperly or unethically acquired).

As noted earlier, however, much of the information available via the Web based search is not available via public view. This information should not be acquired surreptitiously. The ABA Model Rules of Professional Conduct address this issue:

Rule 4.1 Truthfulness in Statements to Others

In the course of representing a client a lawyer shall not *knowingly*:

- (a) make a false statement of material fact or law to a third person; or
- (b) fail to disclose a material fact when disclosure is necessary to avoid assisting a criminal or *fraudulent* act by a client, unless disclosure is prohibited by *Rule 1.6*.

Rule 4.2 Communication With Person Represented By Counsel

In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.

Rule 8.4 (c) Misconduct

It is professional misconduct for a lawyer to:

- (c) engage in conduct involving dishonesty, *fraud*, deceit or misrepresentation.

[http://www.law.cornell.edu/ethics/aba/current/ABA_CODE.HTM#Part percent201 percent20- percent20Client percent20Lawyer percent20Relationship](http://www.law.cornell.edu/ethics/aba/current/ABA_CODE.HTM#Part%201%20-%20Client%20Lawyer%20Relationship). Simply, this means that an attorney and her agents cannot ethically “friend” or connect to an individual represented by counsel if the applicable jurisdiction follows the ABA Model Rules.

The next question becomes what can be done—or how far may one go—when contacting a witness via the Internet. Here the ABA Model Rules of Professional Conduct offer commentary about not being fully candid when contacting a witness:

Rule 4.3 Dealing with Unrepresented Person

In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer *knows* or *reasonably should know* that the unrepresented person misunderstands the lawyer’s role in the matter, the lawyer shall make *reasonable* efforts to correct the misunderstanding. The lawyer shall not give legal advice to an unrepresented person, other than the advice to secure counsel, if the lawyer knows or reasonably should know that the interests of such a person are or have a reasonable possibility of being in conflict with the interests of the client.

A well discussed advisory opinion by the Philadelphia Bar Association Guidance Committee addressed whether an “inquirer” could friend—to make an online connection with someone—a witness in order to gain access to what was believed to be helpful pages on social networking sites that would otherwise be private and inaccessible to the inquirer. After citing to a number of Pennsylvania Rules of Professional Conduct,

the Guidance Committee explained that contacting a witness without full disclosure of the purpose and nature of the contact was improper because it relied upon deceit. http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf; see also, Jinny M. Ray, *Rules Struggle to Catch Up with Technology—Social Networking Ethics*, For The Defense, October 2009, at 72 & 74.

The Philadelphia Bar Association Professional Guidance Committee, though, did note within its advisory opinion that its view was not unanimous within the country and that in certain limited circumstances dissimulation was permissible.

The Committee is aware that there is controversy regarding the ethical propriety of a lawyer engaging in certain kinds of investigative conduct that might be thought to be deceitful. For example, the New York Lawyers' Association Committee on Professional Ethics, [citation omitted] approved the use of deception, but limited such use to investigation of civil right or intellectual property right violations where the lawyer believes a violation is taking place or is imminent, other means are not available to obtain evidence and rights of third parties are not violated.

http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf; see also, the NYCLA Committee on Professional Ethics Formal Opinion No. 737 at http://www.nycla.org/siteFiles/Publications/Publications519_0.pdf.

IV. Where to Look—Issuing Discovery

Searching the Internet for publicly available information is relatively straightforward. Go to Google, Bing, Yahoo! or any search engine, type in your search and voila, off you go. The difficulties seem to arise when the endeavor requires more than a basic search.

In any case involving the potential need to access Web based information formal discovery that addresses the issues should be narrowly crafted and served in the forms of interrogatories, requests to produce, requests to admit and subpoenas. Expect the opposing party to challenge these requests. Before serving discovery or as a part of the initial efforts in a case, sending opposing counsel a litigation hold letter demanding that the information you (intend to) seek be preserved can help to ensure that electronically stored information is not altered. Data changes so quickly on the Web that the information sought may be deleted or changed before the investigating party actually has an opportunity to acquire it via answered discovery or produced responses.

A. Interrogatories

1) Interrogatories should include:

- a) Requests for identification of social networking sites utilized, usernames, identification numbers, URL numbers, other aliases used on the website, and length of time and dates of membership with the site, if appropriate.
- b) Identification of all email and instant messaging addresses and accounts for the party for the relevant time period.
- c) Requests for all search engines utilized.
- d) The IP address for all computers utilized. (An IP address, Internet Protocol address, is used to differentiate computers. Each computer connected to the Internet is assigned at least one unique IP address. This number can vary if the internet service provider utilized does not remain consistent. See, <http://www.chami.com/tips/internet/041498I.html>. Having this

information in hand can make it easier to track the activities and request or subpoena other information.)

- e) The name and address of the Internet Service Provider for the relevant period in question and the applicable account number(s).
 - f) The name and address of the Cell Phone Service Provider for the relevant period in question and the applicable account number(s).
- 2) Requests to Produce should include:
- a) Copies of all searches conducted regarding any issue(s) raised by the plaintiff's complaint and the plaintiff's alleged injuries.
 - b) Copies of home pages for any social network sites of which the party is a member.
 - c) Copies of Internet Service Provider bills for the relevant period.
 - d) Copies of cell phone provider bills for the relevant period.
 - e) Copies of documents maintained or shared by a person on social networking sites, including video and photos.

Subpoenas to Website companies are more difficult to complete. Ideally, any issued discovery should include authorizations or consents for the release of information of the party from social networking sites, internet service providers, cell phone service providers, and email service providers.

The Stored Communications Act prohibits a "person or entity providing an electronic communication service to the public" from knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service. # HYPERLINK "https://www.lexis.com/research/buttonTFLink?_m=997ade664c5c31154ecc350c67cc0466&_xfrcite=percent3ccitepercent20ccpercent3dpercent22USApercent22percent3epercent3cpercent21percent5bCDATApercent5b2009percent20U.S.percent20Dist.percent20LEXISpercent2084176percent5dpercent5dpercent3epercent3cpercent2fcitepercent3e&_butType=4&_butStat=0&_butNum=4&_butInline=1&_butInfo=18percent20U.S.C.percent202701&_fmtstr=FULL&docnum=1&_startdoc=1&wchp=dGLbVzb-zSkAB&_md5=acb165b9c0cfc98eb64c4aa496bf569b" 18 U.S.C. §2701(a)(1).

Thayer v. Chiczewski, 2009 U.S. Dist. LEXIS 84176, *13 (N.D. Ill. 2009). This statute may not apply if a party consents to release or if the court determines that the service was acting more as a secondary storage facility for (electronically created) documents that the party otherwise deleted. Given the number of decisions that have been handed down, it is clear that securing a consent either routinely during the course of a case or with the assistance of the judicial system will ease, assist and speed the release of records. Appendix A offers some guidance for acquiring records from a variety of Web based entities.

Many of the Web companies require that subpoenas be issued and served in California. This means that you may need to domesticate a subpoena. For federal cases this is simple. In federal court, issue a subpoena from the appropriate U.S. District Court in California and require production at a designated location within the state. State court subpoenas require domestication. California recently passed the Interstate and International Depositions Act, Cal. Code Civ. Proc. Section 2029.100, *et seq.*, which is supposed to provide a more detailed explanation of the process. (As of the date of completion of this article the new California law had not yet come into effect.)

V. Discovery and Admissibility

Web based electronically stored information has relatively few reported decisions when compared to its omnipresence in society. Many of the reported decisions involve criminal matters. Even in those cases, it is clear that the information gathered during Internet based discovery and investigation can be utilized in a number of ways.

A. Publicly Displayed Information Has No Expectation of Privacy

Parties cannot claim that the information they post in public fora cannot be utilized in litigation. See *Moreno supra*. Many courts have held that there is no expectation of privacy when it comes to the existence of publically displayed information such as a social networking account. In *Courtright v. Madigan*, the district court for the Southern District of Illinois held that a prisoner had no reasonable expectation that the fact or existence of his MySpace account would remain private. *Courtright v. Madigan*, 2009 U.S. Dist. LEXIS 102544, *7 (S.D. Ill. 2009). In reaching its decision, the district court recited a litany of cases noting that federal courts have unanimously held that a person has no expectation of privacy in Internet subscriber information. *Courtright v. Madigan*, 2009 U.S. Dist. LEXIS 102544, *6 citing to # HYPERLINK "[https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=18& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b412 percent20F. percent20Supp. percent202d percent20174 percent2c percent20181 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=2a4e2ba4c6658f7d6af1ad0647e1210d](https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=17& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b255 percent20F.3d percent20325 percent2c percent20336 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=c032219000df2fcc15c73d0ae7d23108)" *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001); # HYPERLINK "[https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=20& butInline=1& butinfo= percent3ccite percent20cc per-](https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=19& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b400 percent20F. percent20Supp. percent202d percent20843 percent2c percent20848 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=7acbe87cf1d379aa745e3c7302791fc3)

[cent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b190 percent20F. percent20Supp. percent202d percent20330 percent2c percent20332 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=58b08a56f4134e168d1d359f77573d3e](#)” *United States v. Cox*, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002); # HYPERLINK “[https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=21& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b81 percent20F. percent20Supp. percent202d percent201103 percent2c percent201110 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=5153b7756f1d38b4640e11658ad56f4b](#)” *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kans. 2000); # HYPERLINK “[https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=22& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b55 percent20F. percent20Supp. percent202d percent20504 percent2c percent20508 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=b2e7c89ff348ed50090c39b87486aca0](#)” *United States v. Hambrick*, 55 F. Supp. 2d 504, 508-09 (W.D. Va. 1999), *aff’d*, # HYPERLINK “[https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=23& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b225 percent20F.3d percent20656 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=c93bf65472240ead4d564794b59a13ce](#)” 225 F.3d 656 (4th Cir. 2000). #This analysis follows other cases that have held that a person has no reasonable expectation of privacy in information exposed to third parties, like a telephone company or bank. See # HYPERLINK “[https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=24& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b442 percent20U.S. percent20735 percent2c percent20742 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=f6d6e3c28976c263069ac cf3ab8da6f4](#)” *Smith v. Maryland*, 442 U.S. 735, 742, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979) (finding no privacy interest in telephone numbers dialed); # HYPERLINK “[https://www.lexis.com/research/buttonTFLink? m=d9c16c7b37c4a69f6e1dd7ab78cf512c& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent20102544 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=25& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b425 percent20U.S. percent20435 percent2c](#)

[percent20442 percent5d percent5d percent3e percent3c percent2fcite percent3e&fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLzVlz-zSkAW& md5=13ee80b5b20efd47c1e0c8f2b4e66426](#)” *United States v. Miller*, 425 U.S. 435, 442, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976) (finding no privacy interest in bank records).

B. Court Cases Addressing Possible Uses of Web Based Information

Social network site postings can be utilized to show the character of an individual. In *Clark v. Indiana*, the Indiana Supreme Court upheld the use of a MySpace posting of the petitioner by the prosecution during cross-examination to show his character. The petitioner, who had been convicted of murder by the trial court over a defense of intoxication, contended that his postings were neither admissible nor probative. *Clark v. Indiana*, 915 N.E.2d 126, *7 (Ind. 2009). The petitioner wrote on his page:

Society labels me as an outlaw and criminal and sees more and more everyday how many of the people, while growing up, and those who judge me, are dishonest and dishonorable. Note, in one aspect I’m glad to say I have helped you people in my past who have done something and achieved on the other hand, I’m sad to see so many people who have nowhere. To those people I say, if I can do it and get away. B...sh.... And with all my obstacles, why the f... can’t you.”

Id. at *6. The court determined that this posting was not about any act he may have committed but rather was about who the petitioner was as a person. *Id.* at *7.

Evidence gathered from social networking sites can be used to show that a party engaged in activity or behavior contrary to what he has claimed. In *United States v. Villanueva*, the appellate court upheld the use of statements the defendant made while holding an unloaded weapon in a YouTube video and photos of him holding three loaded firearms as a basis for triggering sentencing enhancements. *United States v. Villanueva*, 2009 U.S. App. LEXIS 3852, *8 (11th Cir. 2009).

In another criminal case, prosecutors used posted MySpace photos of the convicted defendant to have three witnesses identify the defendant as someone who had previously threatened them while holding the gun and asking, “Do you want to play?” *People v. Liceaga*, 2009 Mich. App. LEXIS 160, *4 (Mich. Ct. App. 2009). The prosecutors also used the photos to illustrate his familiarity with the weapon involved in the crime. *Id.* at *11-12. The court found no abuse of discretion by the trial court in admitting the photos into evidence.

A Canadian court ordered the production of a hard drive in a civil case so that it could be examined to determine when the plaintiff logged in and out of her Facebook account. *Bishop v. Minichiello*, 2009 BCSC 358 (Supreme Court 2009); <http://www.courts.gov.bc.ca/jdb-txt/SC/09/03/2009BCSC0358.htm>. The plaintiff contended that the production would violate the privacy rights of her family members and friends who also used the computer. The court ruled that the hard drive should be produced as:

[t]he information sought by the defence in this case may have significant probative value in relation to the plaintiff’s past and future wage loss, and the value of production is not outweighed by competing interests such as confidentiality and the time and expense required for the party to produce the documents.

Bishop v. Minichiello, 2009 BCSC at para. 57. To help ensure that confidentiality interests would be protected, the court ordered that an independent expert review the hard drive and segregate out the necessary information. *Id.*

In another civil case, the production of social network postings was ordered, even when the party seeking the information had nothing more than a suspicion that certain postings had occurred. Two minors were denied insurance coverage for treatment for eating disorders. In separate cases the insurer sought the

teenagers' postings in emails, journals, diaries, and communications concerning the minor children's eating disorders or manifestations and symptoms of the eating disorders on any social networking sites that had been shared with the public—even though there was no proof that the minors actually had made any such postings. The cases were consolidated. In response to the insurer's efforts, the families argued that production of the material would harm and hurt the teenagers' recovery. In ordering that the online postings from Facebook and MySpace should be produced the court disagreed finding that "privacy concerns are far less where the beneficiary herself chose to disclose the information." *Beye v. Horizon Blue Cross Blue Shield*, No. 06-Civ.-5377 (D.N.J. 2007); *Foley v. Horizon Blue Cross Blue Shield*, No. 06-Civ.-6219 (D.N.J. 2007).

Illustrating that people do not consider the ramifications of what they post on line, one defendant learned through searches of public portions of social networking websites that plaintiffs had posted information that called into question their claimed damages. The company then issued subpoenas to Facebook, MySpace, and another social networking site, Meetup.Com. The plaintiffs filed Motions for Protective Orders pursuant to Federal Rule of Civil Procedure 26(c) seeking to quash the subpoenas. In *Ledbetter v. Wal-Mart Stores, Inc.*, the federal magistrate denied the motion finding that the plaintiffs had waived their claims to privilege and privacy under Colorado law. *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018 (D. Colo. 2009). As a result, the court held that the "information sought within the four corners of the subpoenas...is reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in this case." *Id.* at *2.

In *Bass v. Miss Porter's School*, the plaintiff sought to stop the production of documents by Facebook in response to a subpoena for postings relating to the allegations contained within the plaintiff's amended complaint. *Bass v. Miss Porter's School*, 2009 U.S. Dist. LEXIS 99916 (D. Conn. 2009). The plaintiff contended that the postings "were irrelevant and immaterial, and...not reasonably calculated to lead to the discovery of admissible evidence." *Id.* at *2. The court disagreed and permitted the production finding that "Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting." *Id.* at *3-4. As a result, the content was relevant and discoverable for both purposes of liability and damages.

C. Effects of the Stored Communications Act (SCA) on Discoverability of Electronically Communicated Information

In *Quon v. Arch Wireless Operating Co.*, police officers filed a Complaint in the district court for the Central District of California alleging, *inter alia*, violations of the SCA and the Fourth Amendment by divulging private communications from their department owned pagers. The district court found that Arch Wireless was a "remote computing service" (RCS) under §2702(a), and that it therefore committed no harm when it released the text-message transcripts to its "subscriber," the City. The U.S. Ninth Circuit Court of Appeals reversed the district court and held that Arch Wireless was an "electronic communication service" (ECS) that provided text messaging service via pagers to the Ontario California Police Department. The court further held that the disclosure of the text messages under the SCA was improper and violated the officers' Fourth Amendment rights to privacy because they had no reasonable expectation that the text messages would be discoverable. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008).

In *Flagg v. City of Detroit*, the plaintiff sued the City of Detroit for the unsolved murder of his father based on laxity in investigation, deliberately ignoring and actively concealing material evidence, and depriving the plaintiff of an opportunity to bring a wrongful death suit against the murderer. The plaintiff, the deceased's minor son, subpoenaed text messages of the investigating officers that were stored by a non-party service provider, SkyTel. The City of Detroit argued that text messages between officers were not discoverable because the SCA wholly precluded the production of electronic communication stored by a non-party service provider. The district court held that the plaintiff *was entitled* to obtain the text messages sent or received by speci-

fied officials or employees of the City of Detroit via a request to produce instead of the chosen method, a subpoena. The court explained that a request for production need not be confined to documents or other items in a party's possession, but instead may properly extend to items that are in that party's control under Fed. R. Civ. P. 34(a)(1). As the City of Detroit had control over the text messages because they were public records even though they were in the possession of SkyTel, the text messages were discoverable regardless of SkyTel's status as an RCS or ECS. *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008).

The receipt of a subpoena in a civil case does not, by itself, authorize the Internet Service Provider to disclose materials under the SCA. In *In Re Subpoena Duces Tecum to AOL, LLC*, the district court held that a civil discovery subpoena for emails and other information relating to the accounts of non-parties was prohibited by federal law and overly broad and possibly in violation of the attorney client privilege. *In Re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 614 (E.D. Va. 2008).

In a more recent decision, the Northern District of Illinois addressed the accessibility of emails that had been deleted by the plaintiff. In *Thayer v. Chiczewski*, the plaintiff filed suit arguing that his constitutional rights had been violated by the City of Chicago Police Department after being arrested while trying to protest the Iraq war. *Thayer v. Chiczewski*, 2009 U.S. Dist. LEXIS 84176 (N.D. Ill. 2009). After limiting the scope of its subpoena to AOL for certain emails from the plaintiff's email account in response to a Motion to Quash granted by the Court, the City moved to compel a response. Both the plaintiff and AOL claimed not to have access to the sought emails, which according to the District Court Judge proved misleading, at best. The district court examined the relevant law in depth:

Plaintiff and AOL have cited numerous cases supporting their position that the SCA prohibits an internet service provider, like AOL, from divulging to a civil litigant the contents of any communication that is carried, maintained, or stored on or by the service. *See, e.g.,* # HYPERLINK "https://www.lexis.com/research/buttonTFLink?_m=997ade664c5c31154ecc350c67cc0466&_xfercite=percent3ccite%20cc%20percent3d%20USA%20percent22%20percent3e%20percent3c%20percent21%20percent5bCDATA%20percent5b2009%20U.S.%20Dist.%20LEXIS%2084176%20percent5d%20percent5d%20percent3e%20percent3c%20percent2fcite%20percent3e&_butType=3&_butStat=2&_butNum=5&_butInline=1&_butInfo=percent3ccite%20cc%20percent3d%20USA%20percent22%20percent3e%20percent3c%20percent21%20percent5bCDATA%20percent5b196%20F.R.D.%2020559%20percent2c%2020561%20percent5d%20percent5d%20percent3e%20percent3c%20percent2fcite%20percent3e&_fmtstr=FULL&docnum=1&startdoc=1&wchp=dGLbVzb-zSkAB&md5=d1f13a761074d22d5c94cd4b4a76ad0d" *Federal Trade Commission v. Netscape Communications Corp.*, 196 F.R.D. 559, 561 (N.D. Cal. 2000); # HYPERLINK "https://www.lexis.com/research/buttonTFLink?_m=997ade664c5c31154ecc350c67cc0466&_xfercite=percent3ccite%20cc%20percent3d%20USA%20percent22%20percent3e%20percent3c%20percent21%20percent5bCDATA%20percent5b2009%20U.S.%20Dist.%20LEXIS%2084176%20percent5d%20percent5d%20percent3e%20percent3c%20percent2fcite%20percent3e&_butType=3&_butStat=2&_butNum=6&_butInline=1&_butInfo=percent3ccite%20cc%20percent3d%20USA%20percent22%20percent3e%20percent3c%20percent21%20percent5bCDATA%20percent5b139%20Cal.%20App.%20204th%20201423%20percent2c%20201448%20percent5d%20percent5d%20percent3e%20percent3c%20percent2fcite%20percent3e&_fmtstr=FULL&docnum=1&startdoc=1&wchp=dGLbVzb-zSkAB&md5=c72343ef05218591090029f24f5dc805" *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1448, 44 Cal. Rptr. 3d 72 (Cal. App. 2006). The Court agrees that, although decisions analyzing the SCA have defined its parameters in sometimes competing ways, most courts have concluded that third parties cannot be compelled to disclose electronic communications pursuant to a civil- as opposed to crimi-

nal—discovery subpoena. See *e.g.*, *In re Subpoena Duces Tecum to* # HYPERLINK “

These holdings are consistent with Congress’s intention, in enacting the SCA, to protect from disclosure private, personal information that happens to be stored electronically. # HYPERLINK “[Theofel v. Farey-Jones, 359 F.3d 1066, 1073-74 \(9th Cir. 2004\).](https://www.lexis.com/research/buttonTFLink? m=997ade664c5c31154ecc350c67cc0466& xfercite= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b2009 percent20U.S. percent20Dist. percent20LEXIS percent2084176 percent5d percent5d percent3e percent3c percent2fcite percent3e& butType=3& butStat=2& butNum=11& butInline=1& butinfo= percent3ccite percent20cc percent3d percent22USA percent22 percent3e percent3c percent21 percent5bCDATA percent5b550 percent20F. percent20Supp. percent202d percent20606 percent2c percent20610 percent5d percent5d percent3e percent3c percent2fcite percent3e& fmtstr=FULL&docnum=1& startdoc=1&wchp=dGLbVzb-zSkAB& md5=3b83c7b4203b56c7282dc020293082a” <i>Id.</i> at 610. “The Privacy Act creates a zone of privacy to protect internet subscribers from having their personal information wrongfully used and publicly disclosed by ‘unauthorized private parties.’” <i>Id.</i> citing S. REP. NO. 99-541, at 3(1986), as <i>reprinted in</i> 1986 U.S.C.C.A.N. 3555, 3557. And it is clear that, at the heart of these decisions, lies the courts’ interest in advancing the legislative intent to protect from unauthorized disclosure electronically-stored documents, which would have otherwise remained private. See, <i>id.</i> citing # HYPERLINK “<a href=)

Thayer v. Chiczewski, 2009 U.S. Dist. LEXIS 84176, **13-15 [footnotes omitted].

The district court then explained that the City only requested the plaintiff's documents that he would have possessed had he not deleted them. The SCA permitted disclosure of documents the plaintiff consents to be produced. As a result the emails could be produced because essentially AOL served as the vehicle for recovery of the relevant emails that were sought that the plaintiff would have had to produce had he not deleted them. *Id.* at *25. From these cases it is clear that acquiring a consent, narrowly crafting the subpoena, and gathering as much information as possible before issuing the request is critical to a successful investigation of on line information.

VI. Jury Duty

Investigation of social network sites is not limited to the parties and witnesses. Searches can be used to investigate prospective and current jurors in order to assess their friendliness and bias.

Attorneys and jury consultants use social networking sites to check the backgrounds of potential and actual jurors. Those who have seen and participated in enough trials know that jurors are not always as candid as they could and should be when answering questions during *voir dire*. Investigating social network sites enables parties to gather information that may be utilized by the trial attorney to craft an argument that might more favorably influence a juror or jurors during the course of the trial. It can also yield information that might be wielded to eliminate jurors who have adverse biases or work to keep those with particular sympathies with one party. Molly McDonough, *Trial Consultants Add Facebook/MySpace to Juror Research Toolbox*, ABA Journal, September 29, 2008; Julie Kay, *Social Networking Sites Help Vet Jurors*, The National Law Journal, August 13, 2008.

In Dayton, Ohio, a prospective juror was removed from a high profile case after he wrote, "Barry Price is sitting in hell 'aka jury duty'" on his Facebook page. The plaintiff's attorney found the posting and advised the court. The court denied the defendants' motion for mistrial. Kimball Perry, *Juror Booted for Facebook Comment*, Dayton Daily News, February 1, 2009.

After a defense verdict a juror apparently searched the Web about the plaintiff, found some less than flattering information and contacted the plaintiff's counsel via email about it. The plaintiff's counsel advised the court and opposing counsel, and the judge investigated the juror's potential misconduct. During his interview of the juror, the judge discovered that after the trial, the juror friended the plaintiff and gained access to the private pages of the plaintiff's Facebook account. The juror insisted that this occurred after the trial had ended. The judge interviewed the jury foreperson who had no recollection of any such information coming to his attention during the trial or deliberations. As a result, despite misgivings about the juror's overall veracity, the judge concluded that there was no misconduct that warranted a new trial. *Wilgus v. F/V Sirius, Inc.*, 2009 U.S. Dist. LEXIS 100094 (D. Maine 2009); see also *United States v. Fumo*, 2009 U.S. Dist. LEXIS 51581, *184-190; 103 A.F.T.R.2d (RIA) 2727 (E.D. Pa. 2009)(finding no basis for an abuse of discretion by failing to overturn a verdict because of juror misconduct after a juror posted comments regarding the trial on his Twitter and Facebook accounts in violation of the court's order not to discuss the trial with anyone).

VII. Service of Process

States often permit substitute service of process when the party trying to complete the service demonstrates that ordinary service is impractical. In New York, two reported decisions have moved the bar and permitted service via electronic means. In *Hollow v. Hollow*, the court held that service upon the defendant's last known e-mail address accompanied by service via international registered air mail and international mail

standard was proper under New York law. *Hollow v. Hollow*, 193 Misc. 2d 691, 696 (N.Y. Sup. Ct. 2002). In a more recent decision, the court authorized service by e-mail that was accompanied by mailing the summons and complaint to the defendant corporations' and president's last known addresses and by calling the president at his last known cellular phone number. *Snyder v. Energy Inc.*, 19 Misc. 3d 954, 963-64 (N.Y. Civ. Ct. 2008).

When parties fail to use the Web and all of its instrumentalities, courts can find that inadequate efforts have been made at achieving service of process. In *Munster v. Groce*, the appellate court held that a "bare-bones affidavit" indicated that due diligence was not used to locate the defendant's whereabouts because there was no indication of among other things, use of the Internet. *Munster v. Groce*, 829 N.E.2d 52, 61 (Ind. Ct. App. 2005). The court went on to note that its simple Google search yielded a result that apparently was not even attempted by the plaintiff. *Id.* at FN 3.

VIII. Texting, Social Networking and the Commercial Transportation Industry

According to the National Highway Transportation Safety Administration (NHTSA), driving while distracted, which includes anything that takes the driver's focus off of the roadway, including using a cell phone and texting, is exceptionally dangerous. "In 2008, 5,870 people lost their lives and an estimated 515,000 people were injured in police-reported crashes in which at least one form of driver distraction was reported on the crash report." "An Examination of Driver Distraction as Recorded in NHTSA Databases," <http://www-nrd.nhtsa.dot.gov/Pubs/811216.PDF>, Sept. 2009. In 2008 NHTSA reported that one percent of all drivers operated their vehicle while "visibly manipulating hand-held devices" and that six percent of all drivers, more than 800,000 people, used hand-held cell phones while driving. <http://www-nrd.nhtsa.dot.gov/Pubs/811184.PDF>.

In response, in October of 2009, the Obama administration said that it will seek to ban text messaging and restrict cell phone use by interstate commercial motor vehicle operators. The Secretary of Transportation, Ray LaHood, also said that the federal government will push states to pass their own laws against driving cars while distracted. <http://www.cbsnews.com/stories/2009/10/01/politics/main5356500.shtml>; <http://www.federalnewsradio.com/?nid=27&sid=1774238>. Numerous states and jurisdictions already have restrictions on cell phone use and texting while driving. For a listing as of November 2009, see Appendix B.

IX. Google Scholar

A new and expanded form of Google Scholar appeared in November of 2009. <http://scholar.google.com/>. Google Scholar now publishes full text legal cases and opinions on line. Google writes:

Google Scholar provides a simple way to broadly search for scholarly literature. From one place, you can search across many disciplines and sources: articles, theses, books, abstracts and court opinions, from academic publishers, professional societies, online repositories, universities and other web sites. Google Scholar helps you find relevant work across the world of scholarly research. <http://scholar.google.com/intl/en/scholar/about.html>.

Google Scholar can be used to access cases, legal journals and a bevy of other academic sources. It does not appear to provide the same depth of content as Lexis or Westlaw and it certainly does not have the same analytic tools. Nonetheless, Google Scholar, like many other search engines, is another tool that can yield different investigative results. It even has the capability of utilizing a reference-like feature that takes the researcher to cited and related sources. The reference component is not anywhere as sophisticated as Shepard's, but it is yet another tool.

Beyond the newly added legal component, Google Scholar is another resource attorneys can use throughout a case. For example, it can be used to find articles written for scholarly publications and it can

help separate some of the wheat from the chaff when searching for works prepared by or materials referencing experts.

X. Conclusion

The Web is another tool in the arsenal of options available to parties before, during and after litigation. Parties that ignore it do so at their peril. The amount of available data is only going to increase and parties must proactively seek the information necessary to complete effective searches. At the same time, companies that do business on the Internet are not going to simply hand over information when it is demanded. Litigants must plan in advance in order to acquire and use web based information.

Appendix A

This Appendix attempts to offer some guidance for acquiring records from various Websites. It is clear that some of these companies are reluctant to turn over information, even when they are required to do so by law. Sections of the various company policies follow as in effect in November of 2009 or at the time of the relevant search. Before relying on this information, it is critical that the searcher check the company's website and other on-line resources before proceeding because the posted information changes so frequently.

I. Facebook

A. Facebook's Privacy Policy Inclusions

To respond to legal requests and prevent harm. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our *Statement of Rights and Responsibilities*. This may include sharing information with other companies, lawyers, courts or other government entities. <http://www.facebook.com/policy.php>.

B. Subpoena Facebook

156 University Avenue
Palo Alto, California 94301
Phone Number: 650-543-4800
Fax Number: 650-644-3229
E-mail Address: subpoena@facebook.com

Facebook requires that a court order for civil matters is obtained through California or New York. Provide Facebook with as much information as possible, including detailed contact information for the person initiating the subpoena so they may follow up on the request. The failure to do so will hinder the success of any endeavor.

Asking Facebook to preserve information yielded the following response. See <http://lawyerist.com/subpoena-facebook-information/>.

Thank you for contacting Facebook.

If you are requesting that information on our site be preserved, please send a preservation order by mail or fax to the following address:

Facebook
1601 S California Avenue
Palo Alto, CA 94304
Attn: Security Department
Fax Number (650) 644-3229

Please provide as much of the following information as possible to expedite your request:

- Your full contact information (name, physical address, phone and email):
- Response date due (please allow 2-4 weeks for processing):
- Full name of user(s):
- Full URL to Facebook profile:
- School/networks:
- Birth date:
- Known email addresses:
- IM account ID:
- Phone numbers:
- Address:
- Period of activity (specific dates will most likely expedite your request):

Please be sure that your contact information is valid, so that we can contact you with updates on your request status.

Although providing this information will enable us to identify the account in question so that we can preserve available information, we will also need a valid subpoena or other court order in order to provide this information to you. This subpoena or court order should be mailed or faxed to the above address.

II. MySpace

MySpace provides detailed information and direction for contacting the company for information on its subscribers. See <http://lawyerist.com/subpoena-myspace-information/>.

A. MySpace Online Service Address

407 N. Maple Drive
 Beverly Hills, California 90210
 USA
 Phone Number: 888-309-1311
 Fax Number: 310-356-3485
 E-mail Address: lawenforcement@myspace-inc.com

MySpace requires personal service of legal requests to its registered agent in Los Angeles.

MySpace requires specific information in order to comply with your legal request. Providing only the user's first and last names or dates of birth is not sufficient to identify the user's profile. MySpace requires the user's unique friend ID number or URL. The friend ID number is located in the URL line. For example, within the URL <http://www.myspace.com/index.cfm?fuseaction=user.viewProfile&friendID=6221&Mytoken=20050518161358>, the friend ID is 6221.

The type of information MySpace can produce in response to a legal request is restricted by federal law. With a subpoena, MySpace may lawfully produce basic subscriber information and IP logs for a user's account. MySpace is prohibited from lawfully producing the contents of a user's private mail messages or stored content files held or maintained on behalf of a user to a any non-government entity, by the Stored Communications Act ("SCA") 18 U.S.C. §§2702-2703. The materials protected from disclosure by Section 2702(a)(2) include MySpace user content including, but not limited to, friend lists, photos, blogs and private messages.

If these records are truly integral to the instant case, the clearly available mechanism for obtaining them is for the owner of the MySpace accounts in question to consent. For civil matters, this consent must be accompanied by a subpoena. To provide proper consent, MySpace requires that a user supply a signed statement containing the friend ID for the account, the password associated with the account, the user's zip code,

and the birth date provided to MySpace. Also obtain an Order from the court compelling the owner of the account to consent to the disclosure of the emails in question.

MySpace requires personal service of subpoenas in civil matters. MySpace will accept personal service at 2121 Avenue of the Stars, Suite 700, Los Angeles, CA 90067 between the hours of 9:30-12:30 and 2:30-5:30. Personal service will also be accepted at CSC locations throughout the state of California. For a list of California locations, please call 888-690-2882. All subpoenas should be addressed to the Custodian of Records for MySpace.com. Additionally, MySpace will only accept subpoenas from out-of-state civil litigants if they have been properly domesticated through a California court.

III. Google

In response to a request for information, Google responded in the following fashion with relatively simple and detailed direction. See <http://tdcaa.infopop.net/2/OpenTopic?a=tpc&s=347098965&f=5340985611&m=6151083251>.

Thank you for your message.

The information you are requesting is subject to state and federal laws.

In accordance with those laws, it is Google's policy to only provide information pursuant to a valid third party subpoena or other appropriate legal process.

If you have additional questions in obtaining such information, please feel free to contact us at legal-support@google.com.

For subpoena requests, please send them to:

Fax: 650-649-2939

Attention: Custodian of Records

Google, Inc.

1600 Amphitheatre Parkway

Mountain View, CA 94043

Sincerely,

Google Legal Investigations Support

The Google privacy policy explains how Google will share personal information. See <http://www.google.com/privacypolicy.html>.

IGoogle's Privacy Policy

Information sharing

Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:

- We have your consent. We require opt-in consent for the sharing of any sensitive personal information.
- We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.
- We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues,

or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.

IV. AOL

As noted within earlier sections, AOL has been involved in its fair share of litigation. AOL provides detailed information of the records acquisition process. That being noted one district court wrote, “AOL states, repeatedly, that it receives over 350 civil subpoenas each year. So, when AOL received the City’s two subpoenas, it raised its standard objection that AOL does not divulge emails to a third party in response to a civil subpoena.” *Thayer v. Chiczewski*, 2009 U.S. Dist. LEXIS 84176, *10. In a footnote the court added, “The letter does not explain, however, why 350 subpoenas would so cripple a multi-billion dollar corporation with over 6,000 employees that it resorts to ignoring court orders and proffering incomplete and inaccurate information, which has compounded costs and unnecessarily delayed this litigation.” *Thayer v. Chiczewski*, 2009 U.S. Dist. LEXIS 84176, *9.

The AOL policy regarding privacy and disclosure of information of its account holders follows. See <http://legal.web.aol.com/aol/aolpol/civilsubpoena.html>.

AOL is committed to protecting the privacy of its account holders. According to AOL’s *Terms of Service*, including its *Privacy Policy*, AOL will not release the content of account holder e-mail until AOL has sent notification to the account holder and in all but the rarest of cases, *only with the valid consent of the account holder*. Our authorization form can be found *here*. Because free email accounts cannot be properly verified [through address and payment information], we will not release email content of free AOL accounts, even to the account holder. However, in its ordinary course of business, AOL retains no active account holder email that is not also accessible by the user. Parties are therefore encouraged to request the information they are seeking through the AOL account holder.

Account information that does not include email content, such as identifying information, may be released in connection with a valid civil subpoena.

Valid Civil Subpoena Process (for account holder information or information sufficient to identify an account holder only):

AOL, its records, and its Custodian of Records are located in Loudoun County, Virginia. AOL’s headquarters are in the State of New York. AOL accepts subpoenas that are properly issued pursuant to Federal Rule of Civil Procedure 45 and applicable state laws.

For all properly issued subpoenas, service should be made upon our registered agent:

Corporation Service Company
11 South 12th Street
Post Office Box 1463
Richmond, Virginia 23218

Upon receipt of a valid subpoena, it is AOL’s policy to promptly send notification to the account holder whose information is sought. AOL will not produce the subpoenaed account holder information until 10 days after the account holder has been notified, so that the account holder whose information is sought will have adequate opportunity take appropriate legal action, should the account holder wish to do so. AOL will issue invoices for the costs associated with subpoena compliance. We charge \$125.00 per hour for research and administrative costs, \$14.00 per overnight mail and 25 cents per copy. AOL will invoice the subpoenaing party prior to production, and payment *must* be made prior to the production of the subpoenaed information.

Account holder E-mail and Content

AOL will not release the content of account holder e-mail until AOL has sent notification to the account holder and, in all but the rarest of cases, *only with the valid consent of the account holder*. Our authorization form can be found *here*. As noted above, because free email accounts cannot be properly verified through address and payment information, AOL will not release email content of free AOL accounts, even to the account holder.

Pursuant to the Stored Wire and Electronic Communications Act (Stored Communications Act), 18 U.S.C. §2701 et seq., AOL will not release an account holder's e-mail content even with a properly issued subpoena or a court order. See, *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606 (E.D. Va. 2008) (A civil discovery subpoena is not an exception to the provisions of the Privacy Act that would allow an internet service provider to disclose an Account holder's email. The exception for production pursuant to court order does not apply to civil discovery matters.); *Flagg v. City of Detroit*, 2008 WL 3895470 (E.D. Mich. 2008) (“[The Stored Communications Act] lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to subpoena or court order.”).

Moreover, in its ordinary course of business, *AOL retains no active account holder email that is not also accessible by that account holder*. Therefore, if a party is seeking account holder email, the most efficient way to access that information is through the account holder.

AOL will issue invoices for the costs associated with subpoena compliance. We charge \$125.00 per hour for research and administrative costs, \$14.00 per Federal Express and 25 cents per copy. AOL will invoice the subpoenaing party prior to production, and payment *must* be made prior to the production of the subpoenaed information.

Note, in *Thayer v. Chiczewski*, the Northern District Court of Illinois determined after reviewing the defendant's expert's affidavit that the representation that AOL retained no account holder email that was not also accessible by the account holder to be inaccurate. The court indicated that such information should have been available on the company's disaster recovery system. *Thayer v. Chiczewski*, 2009 U.S. Dist. LEXIS 84176, *24.

V. Yahoo!

The Yahoo! information sharing and privacy policy follows. See <http://info.yahoo.com/privacy/us/yahoo/details.html>.

Information Sharing and Disclosure

Yahoo! does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

- We provide the information to trusted partners who work on behalf of or with Yahoo! under confidentiality agreements. These companies may use your personal information to help Yahoo! communicate with you about offers from Yahoo! and our marketing partners. However, these companies do not have any independent right to share this information.
- We have a parent's permission to share the information if the user is a child under age 13. Parents have the option of allowing Yahoo! to collect and use their child's information without consenting to Yahoo! sharing of this information with people and companies who may use this information for their own purposes.

- We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims.
- We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo!’s terms of use, or as otherwise required by law.
- We transfer information about you if Yahoo! is acquired by or merged with another company. In this event, Yahoo! will notify you before information about you is transferred and becomes subject to a different privacy policy.

Yahoo! displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click targeted ads meet the targeting criteria—for example, women ages 18-24 from a particular geographic area.

- Yahoo! does not provide any personal information to the advertiser when you interact with or view a targeted ad. However, by interacting with or viewing an ad you are consenting to the possibility that the advertiser will make the assumption that you meet the targeting criteria used to display the ad.
- Yahoo! advertisers include financial service providers (such as banks, insurance agents, stock brokers and mortgage lenders) and non-financial companies (such as stores, airlines, and software companies).

Yahoo! works with vendors, partners, advertisers, and other service providers in different industries and categories of business. For more information regarding providers of products or services that you’ve requested please read our detailed *reference links*.

If you are seeking to obtain the account information we may have regarding a specific subscriber, we will need a subpoena or a court order.

If you have obtained a subpoena or a court order for the release of information regarding a Yahoo! member or visitor, please direct it to:

Custodian of Records
 Yahoo! Inc.
 701 First Avenue
 Sunnyvale, CA 94089

VI. Twitter

Twitter is one of the most popular and fastest growing means of communication. Twitter advises its users:

Law and Harm: We may disclose your information if we believe that it is reasonably necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issues; or to protect Twitter’s rights or property. <https://twitter.com/tos>.

Twitter offers the following for acquiring information maintained by the company (<http://help.twitter.com/forums/26257/entries/41949>):

What user information does Twitter have?

Most Twitter profile information is public, so everyone can see it. A Twitter profile contains a profile image, background, and the status updates, or “tweets” of the account owner. In addition, the user has the option to fill out location, include a URL, and write a “one line bio” or short phrase about themselves. The tweets on a profile page update in real time, so the newest information is

always available at the top. Public profiles also show a list of whose tweets the account owner “follows” or subscribes to, as well as the account owner’s “followers” or, those who subscribe to the tweets of the account owner.

Private information requires a subpoena or court order

In accordance with our *Privacy Policy* and *Terms of Service*, non-public information about Twitter users is not released unless we have received a subpoena, court order, or other legal process document. Some information we store is automatically collected, while other information is provided at the user’s discretion. Though we do store this information, it may not be accurate if the user has created a fake or anonymous profile. Twitter doesn’t require email verification or identity authentication.

Data retention information

Twitter retains different information for different time periods. Twitter may retain user information longer than usual in the case of preservation requests. Data preservation requests must be accompanied by a subpoena or court order. Preservation requests must be signed and sent on law enforcement letterhead. Requests may be sent via the methods described below, and unless otherwise required, the user will still have access to their account.

How to request user information with a subpoena or court order

Twitter accepts subpoenas delivered by mail or fax. In order to expedite the process, subpoenas should include the URL of the Twitter profile in question, and details about what specific information is required. Twitter conducts most correspondence via email, so please include an email contact so we may contact you. To contact us, email: lawenforcement@twitter.com.

Only email from law enforcement domains is accepted. Non-law enforcement requests should be sent through our regular support methods. Non-law enforcement mail will be deleted.

The Twitter address is:

Twitter, Inc.

795 Folsom St., Suite 600

San Francisco, CA 94107

It is impossible to identify and list every search engine, hosting site, social networking site or generally everything of anything that is on the Web. One good reference tool is one relied upon by law enforcement called the ISP List, <http://www.search.org/programs/hightech/isp/default.asp#212>. According to its own description, it “contains a variety of ISPs and similar information services, specifically, contacts at the legal departments for law enforcement service of subpoena, court orders, and search warrants.”

Appendix B

The following table was created by the Insurance Institute for Highway Safety—<http://www.iihs.org/laws/cellphonelaws.aspx>. It lists laws restricting cell phone use and texting while driving as of November 2009.

Laws Restricting Cell Phone Use And Texting

State	Hand-Held Ban	Young Drivers	All Cell Phone Ban	Bus Drivers	All Cell Phone Ban	Texting
<i>Ala.</i>	N	N	N	N	N/A	
<i>Alaska</i>	N	N	N	All drivers	Primary	
<i>Ariz.</i>	N	N	School bus drivers	N	Primary	
<i>Ark.</i>	Drivers ages 18-20	Drivers younger than 18	School bus drivers	All drivers	Primary: texting by all drivers and cell phone use by school bus drivers; secondary: cell phone use by young drivers	
<i>Cal.</i>	All drivers	Drivers younger than 18	School and transit bus drivers	All drivers	Primary; secondary for hands-free cell phone use by young drivers	
<i>Colo.</i>	N	Drivers younger than 18 (effective 12/01/09)	N	All drivers (effective 12/01/09)	Primary (effective 12/01/09)	
<i>Conn.</i>	All drivers	Drivers younger than 18	School bus drivers	All drivers	Primary	
<i>Del.</i>	N	Learner's permit and intermediate license holders	School bus drivers	Learner's permit and intermediate license holders	Primary	
<i>D.C.</i>	All drivers	Learner's permit holders	School bus drivers	All drivers	Primary	
<i>Fla.</i>	N	N	N	N	N/A	
<i>Ga.</i>	N	N	School bus drivers	N	Primary	
<i>Haw.</i>	N	N	N	N	N/A	
<i>Idaho</i>	N	N	N	N	N/A	
<i>Ill.</i>	Drivers in construction and school speed zones (eff. 01/01/10)	Drivers younger than 19 and learner's permit holders younger than 19	School bus drivers	All drivers (eff. 01/01/10)	Primary	
<i>Ind.</i>	N	Drivers younger than 18	N	Drivers younger than 18	Primary	
<i>Iowa</i>	N	N	N	N	N/A	

<i>Kan.</i>	N	Learner's permit and intermediate license holders (eff. 01/01/10)	N	Learner's permit and intermediate license holders (eff. 01/01/10)	Primary (effective 01/01/10)
<i>Ky.</i>	N	N	School bus drivers	N	Primary
<i>La.</i>	With respect to novice drivers, see footnote	With respect to novice drivers, see footnote	School bus drivers	All drivers	Secondary; primary for school bus drivers
<i>Me.</i>	N	Learner's permit and intermediate license holders	N	Learner's permit and intermediate license holders	Primary
<i>Md.</i>	N	Learner's permit and intermediate license holders	N	All drivers	Secondary; primary for texting
<i>Mass.</i>	Local option	N	School bus drivers	N	Primary
<i>Mich.</i>	Local option	N	N	N	N/A
<i>Minn.</i>	N	Learner's permit holders and provisional license holders during the first 12 months after licensing	School bus drivers	All drivers	Primary
<i>Miss.</i>	N	N	N	Learner's permit and intermediate license holders	Primary
<i>Mo.</i>	N	N	N	Drivers 21 and younger	Primary
<i>Mont.</i>	N	N	N	N	N/A
<i>Neb.</i>	N	Learner's permit and intermediate license holders younger than 18	N	Learner's permit and intermediate license holders younger than 18	Secondary
<i>Nev.</i>	N	N	N	N	N/A
<i>N.H.</i>	N	N	N	All drivers (eff. 01/01/10)	Primary (eff. 01/01/10)
<i>N.J.</i>	All drivers	Learner's permit and intermediate license holders	School bus drivers	All drivers	Primary
<i>N.M.</i>	Local option	N	N	N	N/A
<i>N.Y.</i>	All drivers	N	N	All drivers	Primary; secondary for text messaging

<i>N.C.</i>	N	Drivers younger than 18	School bus drivers	All drivers (eff. 12/01/09)	Primary
<i>N.D.</i>	N	N	N	N	N/A
<i>Ohio</i>	Local option	N	N	N	N/A
<i>Okla.</i>	N	N	N	N	N/A
<i>Or.</i>	All drivers (eff. 01/01/10)	Drivers younger than 18 (eff. 01/01/10)	N	All drivers (eff. 01/01/10)	Primary (eff. 01/01/10)
<i>Pa.</i>	Local option	N	N	N	N/A
<i>R.I.</i>	N	Drivers younger than 18	School bus drivers	All drivers	Primary
<i>S.C.</i>	N	N	N	N	N/A
<i>S.D.</i>	N	N	N	N	N/A
<i>Tenn.</i>	N	Learner's permit and intermediate license holders	School bus drivers	All drivers	Primary
<i>Tex.</i>	Drivers in school crossing zones	Intermediate license holders for the first twelve months	Bus drivers when a passenger 17 and younger is present	Bus drivers when a passenger 17 and younger is present; intermediate license holders for first twelve months; drivers in school crossing zones	Primary
<i>Utah</i>	all drivers	N	N	All drivers	Primary for texting; secondary for talking on a hand-held cell phone
<i>Vt.</i>	N	N	N	N	N/A
<i>Va.</i>	N	Drivers younger than 18	School bus drivers	All drivers	Secondary; primary for school bus drivers
<i>Wash</i>	All drivers	N	N	All drivers	Secondary
<i>W. Va.</i>	N	Drivers younger than 18 who hold either a learner's permit or an intermediate license	N	Drivers younger than 18 who hold either a learner's permit or an intermediate license	Primary
<i>Wis.</i>	N	N	N	N	N/A
<i>Wyo.</i>	N	N	N	N	N/A

Note: The laws in Arkansas and California prohibit police from stopping a vehicle to determine if a driver is in compliance with the law. Clearly, that language prohibits the use of checkpoints to enforce the law,

but it has been interpreted as the functional equivalent of secondary provisions that typically state the officer may not stop someone suspected of a violation unless there is other, independent, cause for a stop.

In Louisiana as of July 1, 2008, all learner's permit holders, irrespective of age, and all intermediate license holders were prohibited from driving while using a hand-held cell phone and all drivers younger than 18 were prohibited from using any cell phone. Effective April 1, 2010 all drivers, irrespective of age, issued a first driver's license will be prohibited from using a cell phone for one year.

Utah's law defines careless driving as committing a moving violation (other than speeding) while distracted by use of a hand-held cell phone or other activities not related to driving.

[Return to course materials table of contents](#)