McGeorge Law Review

Volume 41 | Issue 4 Article 4

1-1-2009

Your Opponent Does Not Need a Friend Request to See Your Page: Social Networking Sites and Electronic Discovery

Derek S. Witte
Cooley Law School

Your Opponent Does Not Need a Friend Request to See Your Page: Social Networking Sites and Electronic Discovery

Derek S. Witte*

I. INTRODUCTION

With each passing year, the technology of how we communicate progresses at an increasingly rapid rate. Thus, it is no surprise that the law—which is still controlled in large part by practitioners, judges, and scholars, who began practicing in the world of hard-copy memoranda and pen-on-paper signatures—continues to lag behind. Our slow reaction to technological change is also attributable to the frustratingly long time it takes to resolve disputes in court. While the world is changing by the minute, the common law system still relies on cases that take years to develop, litigate, and appeal.

Whatever the reason, the law struggles to keep pace with contemporary life. After corporate email went mainstream, respected lawyers still argued that their clients did not need to hand over email and electronic records as part of discovery, because these records were not actually "documents," having never been printed out in hard-copy.[1] Were that not troubling enough, the Supreme Court did not amend the Federal Rules of Civil Procedure to address the discoverability of electronically stored information (ESI) until 2006, over a decade after email became prevalent.

Now, just as the law (although perhaps not the *practice* of the law) has arguably caught up to email and the technology of the 1990s, judges, practitioners, and parties are faced with even newer technology and ever-changing modes of communication.

It should be no surprise, then, that the law provides little guidance on how we should deal with some of the newest sources of evidence: social networking sites, such as the ubiquitous, and some would say pernicious, Facebook. I will do my best to pose the questions that should be asked when parties seek, or seek to protect, the contents of a Facebook or social networking page, such as:

---

* Professor Derek S. Witte teaches Contracts and Commercial Law at Cooley Law School in Grand Rapids, Michigan. Professor Witte is responsible for presenting at the Michigan Institute of Continuing Legal Education on e-discovery. He recently spoke at the International Quality and Productivity Center's 8th E-Discovery Conference in New York on the topic of Facebook and electronically stored information. He has spoken about e-discovery for the Federal Bar Association's West Michigan Chapter and recently moderated and hosted an e-discovery conference for the Grand Rapids Bar Association, which focused on the new Michigan e-discovery rules. Before teaching, Professor Witte provided litigation and consulting support for many private companies and litigants in the area of e-discovery while in private practice.

1. Crown Life Ins. Co. v. Craig, 995 F.2d 1376, 1382 (7th Cir. 1993) ("[Plaintiff] also argues that the data is not 'documents' because it was never in hard copy form . . . .").

1. Are the contents of a social networking page ESI and thus subject to the laws of discovery and spoliation?
2. Must a social networking site, like Facebook, comply with a valid subpoena?
3. How should the law change to balance a litigant's right to access the potentially rich sources of evidence stored on an individual's social networking page with an individual's right to privacy?

This Article suggests some answers to these questions based upon the handful of cases in which courts have faced these emerging issues. However, even as I write this, I fear that by the time the law has caught up with social networking sites, Facebook will be yesterday's news. By then, we will already be reacting to the next technological advancement and struggling with unforeseen sources of ESI and evidence.

II. YOUR FACEBOOK PAGE IS ESI

It seems that many businesses and individuals either do not believe or have not even asked themselves whether the contents of someone's social networking page constitutes ESI that can be discovered and used as evidence in a lawsuit.[2] Perhaps this is because Facebook pages are not stored on individual computers, but are kept by Facebook or the social networking sites themselves.[3] Given that the contents of these pages are stored on someone else's servers, perhaps some people have assumed that these pages are not discoverable ESI, but instead simply another website on the Internet, like nytimes.com or weather.com.[4] This is not the case. In fact, the plain meaning of "ESI," as defined in the federal rules, unquestionably covers the contents of a social networking page, if relevant.[5]

According to Federal Rule of Civil Procedure 34, "ESI" includes "any . . . writings, drawings, graphs, charts, photographs, sound recordings, images, and other *data or data compilations—stored in any medium* from which information

2. Ari Kaplan, *IQPC Puts a Wrap on E-Discovery 2009*, L. TECH. NEWS, Dec. 21, 2009, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202436704025 (on file with the *McGeorge Law Review*) (noting that social networking sites are only relevant to discovery from a "marketing standpoint . . . but not from an ESI standpoint").

3. Another reason that some practitioners may believe that social networking pages are not discoverable ESI is because they believe that privacy laws, such as the federal Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2000), protect their Facebook pages. I will address this below. However, these laws do not shield social networking pages from discovery.

4. The idea that Internet surfing is simply a one-way activity through which the computer user gathers information by visiting static and fixed websites, like reading a magazine, is also a misconception. Most sites store cookies on our computers, which may track and report our Internet activity or simply save files on our computer to make subsequent Internet-surfing quicker and easier. Those cookies themselves are ESI and might be discoverable if relevant. *See infra* notes 6-7 and accompanying text.

5. FED. R. CIV. P. 34(a)(1).

can be obtained . . . ."[6] When the committee responsible for revising the Federal Rules of Civil Procedure drafted the 2006 e-discovery amendments, it intended this definition to be broad so that it would encompass all forms of current and future ESI. The committee stated: "The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically."[7] For this reason, and in light of several recent cases, there should be no dispute that the contents of social networking sites are ESI.[8]

III. SOCIAL NETWORKING SITES PROVIDE FERTILE GROUND FOR HARVESTING ESI

Given that social networking sites are ESI and should be discoverable if relevant in any civil or criminal lawsuit, these sites promise to be a treasure trove of evidence and admissions. Essentially, millions of Americans voluntarily keep detailed journals of their daily thoughts and activities and then send them out into the information vortex of the Internet for viewing and comment.[9] Were that not enough, most believe that these sites are private—adding to the candid nature of their posts, messages, and photographs. From a trial attorney or prosecutor's viewpoint, these pages may be the single richest source of evidence regarding an individual's thoughts and actions available today.

Most social networking sites, such as Facebook, contain the following: biographical information about the account holder (and links to the biographical information of his or her friends); statements and admissions, such as descriptions of "last night" posted to someone's Facebook "Wall," a forum in which both an account-holder and his or her "friends" can post comments; photographs; emails (most social networking sites also provide a fully embedded web-based email program through which members can communicate); instant messages through which members can chat live; and the user's contacts and lists of "friends" or business contacts (such as on the social networking site, LinkedIn).

---

6. *Id.* (emphasis added).

7. FED. R. CIV. P. 34(a) advisory committee's note on 2006 amendment.

8. Bass v. Miss Porter's School, No. 3:08cv1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009) (noting that plaintiff was required to produce 750 pages of materials from her Facebook page, which Facebook provided, including "wall postings, messages, and pictures"); Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009) (stating that information from Facebook and MySpace was properly within a Rule 45 subpoena); *see also* Steven C. Bennett, *Look Who's Talking: Legal Implications of Twitter Social Networking Technology*, 81 N.Y. ST. B.J. 10 (May 2009) (suggesting that contents of a Twitter page are ESI); Sharon D. Nelson et al., *Capturing Quicksilver: Records Management for Blogs, Twittering & Social Networks*, 32 WYO. LAW. 56, 57 (June 2009) (arguing that Tweets are ESI).

9. Seth P. Berman et al., *Web 2.0: What's Evidence Between "Friends"*, 53 BOSTON B.J. 5, 5-6 (Feb. 2009).

For instance, in *Bass v. Miss Porter's School*, the United States District Court for the District of Connecticut ordered the plaintiff to produce "wall postings, messages, and pictures" from her historical Facebook page.[10] The court held that the contents of the page were relevant to the plaintiff's Internet-bullying claims and the defendant's defenses.[11] In another example, a defendant in a forcible rape case tried to admit the victim's statements from her Facebook page about both her drinking habits and her injuries on the night the crime was committed.[12] Although the evidence was suppressed and the appellate court upheld the decision, the case still demonstrates how a Facebook user's statements can become discoverable admissions in a lawsuit—civil or criminal.[13]

In addition to the more obvious types of ESI that users store on social networking pages, the sites themselves may track and store an entire hidden category of potentially discoverable ESI: metadata about their users. These sites track information about their customers' usage of the site, the identities of their "friends" and contacts, and perhaps even their general Internet use.[14] As two technology attorneys describe one such site, "[e]ssentially an entire new aisle of buckets where relevant communications may lie comes to the forefront. . . . The social networking aspects of Web 2.0 connect you to other users, who are in turn connected to other users. This is the network."[15] However, "only the system knows who the second and third degree connections are, not the user."[16]

If captured and recovered, this metadata could establish what a user knew or saw on another webpage or what others saw on the user's social networking page. Such information about viewing patterns could be relevant in all sorts of litigation, such as providing evidence of "knowledge" or "intent" in a criminal or tort case, someone's relationship status in a divorce proceeding where there are allegations of infidelity, or perhaps "publication" in a defamation case.

Social networking sites are also fertile grounds for discovering relevant ESI, because their users speak and write casually. Users may speak candidly, because often they are led to believe that their social networking pages are private.[17] Users are informal, because "electronic communication has a spontaneity that makes it seem impermanent" and casual.[18] This informality is encouraged by the false sense of security created by "private" pages. Even the *New York Times* has

---

10. 2009 WL 3724968, at *1.

11. *Id.*

12. State v. Corwin, 295 S.W.3d 572, 577 (Mo. Ct. App. 2009).

13. *See id.* at 577, 579.

14. *See* Lane v. Facebook, Inc., No. C 08-3845 RS, 2009 WL 3458198, at *1 (N.D. Cal. Oct. 23, 2009) (describing the now discontinued "Beacon program," through which Facebook tracked its users' activity on forty-four other websites and then "post[ed] the information on the member's Facebook 'wall'").

15. Dan Regard & Tom Matzen, *Web 2.0 Collides with E-Discovery*, L. TECH. NEWS, May 30, 2008, http://www.law.com/jsp/PubArticle.jsp?id=1202421780523 (on file with the *McGeorge Law Review*).

16. *Id.*

17. Berman et al., *supra* note 9, at 6.

18. *Id.*

reported that because Facebook "offers a slew of privacy controls . . . *you'll never have to worry . . . .*"[19]

Unfortunately, even a private page is only private from other viewers so long as Facebook, or some other social networking site, chooses to adhere to its own privacy policies and so long as the Facebook user has not been subpoenaed or served with discovery requests as a party in litigation. In other words, Facebook's privacy settings cannot protect you from a valid discovery request seeking the contents of your Facebook page if your page is potentially relevant to the allegations in the lawsuit. Moreover, your duty to produce the contents of your page may still exist even if you have updated your page since the events at issue occurred. In *Bass v. Miss Porter's School*, the producing party had deleted her Facebook page and terminated her account, yet Facebook still kept and released to her 750 pages of information from her historical postings on Facebook, which she was compelled to produce to the defendant.[20]

IV. SO, YOU MUST PRESERVE AND PRODUCE THE CONTENTS OF YOUR PAGE

Because the contents of most social networking sites are indeed ESI, it naturally follows that the rules of preservation, production, and spoliation should apply to the contents of your page. This could have far-reaching implications in litigation. This could mean that if you update your Facebook page when you know that it may contain potentially relevant to foreseeable litigation, you may be spoliating evidence.

To date, no published opinion that this author could find has held that the destruction or loss of one's social networking page while its content are potentially relevant to foreseeable or ongoing litigation could lead to sanctions. However, one decision, *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, has indirectly held that this may be the case.[21] Although the *Mackelprang* court held that MySpace was not required to hand over the plaintiff's MySpace emails, it stated in dicta that, if the MySpace page contents were truly created by the plaintiff, then she may be required to hand them over or face sanctions for failing to do so.[22]

In *Mackelprang*, the defendant in a sexual harassment case subpoenaed emails from a MySpace account allegedly created by the plaintiff.[23] MySpace

---

19. Sarah Perez, *5 Easy Steps to Stay Safe (and Private!) on Facebook*, N.Y. TIMES, Sept. 16, 2009 (emphasis added).

20. No. 3:08cv1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009).

21. No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, at *8 (D. Nev. Jan. 9, 2007) ("[A] refusal by Plaintiff to produce relevant and discoverable email communications based on a wrongful and bad faith denial that the Myspace.com accounts belong to her could be grounds for imposing sanctions.").

22. *Id.* at *8-9.

23. *Id.* at *2.

refused to fully comply.[24] The court held that the requesting party, the defendant, could not establish that the emails were relevant even if MySpace produced them.[25] However, the court noted that if the defendant could properly serve the plaintiff, rather than a third party, with discovery requests for relevant emails, the plaintiff's failure to provide emails from the MySpace account "could be grounds for imposing sanctions."[26]

Although at first glance this appears to be an unimportant decision in which the court simply refused to require MySpace to produce information about the plaintiff, upon closer inspection, this holding was remarkable, because the court: (1) indirectly holds that the contents of a party's social networking page can be discoverable ESI; and (2) places the duty on the account-holder to preserve and produce the contents of her social networking page or face sanctions for failing to do so.[27] Although the court does not state exactly why the ESI could not be subpoenaed directly from MySpace,[28] it did clearly hold that "[t]he proper method for obtaining such information, however, is to serve upon *Plaintiff* properly limited requests for production" of relevant MySpace emails.[29] Further, the court is unequivocal that the plaintiff's failure to produce the contents and email from her MySpace page "could be grounds for imposing sanctions."[30]

The most troubling part of this holding is that the court seems to place the duty to preserve and produce the contents of one's page on the computer-user or account-holder. Yet, the information on a Facebook or other social networking page is stored on the social networking site's servers and storage devices and thus is not completely in the control of the account-holder, at least not to the same extent as files stored directly on his or her computer.[31] The *Mackelprang* court nonetheless assumes that a social networking site customer must have the power to preserve and produce the contents of her own page, even though the information on her site is stored remotely on servers outside of her control.[32]

It seems especially odd to place the duty to preserve and produce the contents of someone's social networking page on the individual computer-user when, after she has updated her page or terminated her account, she has no idea what information the website has retained relating to her historical web pages. For instance, in *Bass v. Miss Porter's School*, Facebook actually retained and

---

24. *Id.*

25. *Id.* at *6.

26. *Id.* at *8.

27. *Mackelprang*, 2007 WL 119149, at *8.

28. As discussed below, some courts have held that the federal Stored Communications Act prevents some webmail providers from producing emails. However, no cases have yet applied the Act to social networking sites.

29. *Mackelprang*, 2007 WL 119149, at *8 (emphasis added).

30. *Id.*

31. *See* Berman, *supra* note 9, at 6 ("Web 2.0 data, like all data on the World Wide Web, typically can be found . . . on the server of the website where the data was posted.").

32. *See id.*

produced 750 printed pages of information containing the producing party's historical postings and Facebook page information, despite the fact that the user had terminated her Facebook account nearly nine months earlier.[33] Many Facebook users would be surprised to learn that Facebook keeps so much historical information about their old pages. Thus, it seems absurd that somehow the account-holder would still be responsible for producing such information.

Further, even if the *Mackelprang* decision were read to place the duty to preserve and produce one's page on an individual user, the social networking sites often will not even cooperate with an account-holder's request for *his own* archived pages. For instance, in the case of *In re Skerry*, Facebook required a formal subpoena before it would release to the petitioner documents related to his personal Facebook account.[34] This was especially problematic for Mr. Skerry, given that he was accused of criminal harassment and believed that someone had tampered with his account.[35] Because no criminal complaint or indictment had yet been filed, Facebook refused to give him his own records.[36]

Given that the contents of a social networking site are ESI and in light of the opinion in *Mackelprang*, there is reason to expect that other courts may impose sanctions for spoliation of ESI if and when a requesting party establishes that the producing party posted potentially relevant information on his or her Facebook, LinkedIn, or MySpace page and subsequently either destroyed, lost, or failed to produce the contents of that page during litigation. Unfortunately, should the courts hold that the account-holders, and not the social networking sites themselves, are ultimately responsible for preserving and producing the contents of these pages, then justice demands that there must be some way for the users to instruct the sites to preserve a user's historical information once a lawsuit becomes foreseeable.

V. IT IS UNCLEAR WHETHER SOCIAL NETWORKING SITES MUST COMPLY WITH ALL VALID CIVIL SUBPOENAS

Because an individual Facebook or LinkedIn customer does not have direct access to the servers upon which his or her pages are stored, much less access to his or her historical or archived page information, it follows that the best way to discover this potentially rich ESI in a civil lawsuit is by requesting it directly from the sites themselves. It is thus no surprise that since these sites have grown in popularity, civil litigants have begun subpoenaing the contents of their opponents' social networking pages directly from Facebook, MySpace, and

33. Bass v. Miss Porter's School, No. 3:08cv1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009).

34. *In re* Skerry, No. C-09-80070 MISC CRB (EMC), 2009 WL 1097326, at *1 (N.D. Cal. Apr. 20, 2009).

35. *Id.* at *1-2

36. *See id.*

others.[37] The enforceability of civil subpoenas is also important, because it appears that most social networking sites will not even release information and documents to a customer about his or her own page absent a subpoena.[38]

Consequently, in the future, the discoverability of ESI created and stored on an individual's social networking page may depend upon a party's ability to enforce a third-party subpoena against the social networking sites themselves. When analyzing this issue, it makes sense for us to separate social networking site subpoenas into three categories: (1) civil subpoenas in which a party requests information from a social networking site relating to *another* customer's account; (2) subpoenas and requests from the government in a criminal action; and (3) civil subpoenas from customers seeking the contents of their own social networking pages.

A. *The Federal Stored Communications Act May Prohibit Enforcement of Civil Subpoenas Requesting Someone Else's Social Networking Page Information*

At least one court has enforced a third-party subpoena from a litigant who requested the contents of an opponent's Facebook or social networking site page.[39] In a terse order, a Magistrate Judge for the United States District Court for the District of Colorado held that a subpoena from Wal-Mart served directly on Facebook and MySpace, in which Wal-Mart sought information from the plaintiffs' social networking pages for Wal-Mart's defense to plaintiffs' claims for injuries relating to an electrical accident, was indeed enforceable.[40]

Despite this decision, however, there may be an argument that, as with web-based email providers, the federal Stored Communications Act (the Act) might actually prohibit social networking sites from divulging any information about a customer's page other than to the customers themselves or to the government in a criminal matter. The Act provides that:

> (1) a person or entity providing *an electronic communication service* to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

---

37. *See, e.g.*, Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *1 (D. Colo. Apr. 21, 2009) (noting that the defendant subpoenaed contents of plaintiffs' accounts from Facebook, MySpace, and Meetup.com relating to its defenses to personal injury claims); *Bass*, 2009 WL 3724968, at *1 ("Plaintiff . . . served a subpoena on Facebook in an attempt to get records of her former Facebook account . . . ."); J.T. Shannon Lumber Co. v. Gilco Lumber, Inc., No. 2:07-CV-119, 2008 WL 3833216 (N.D. Miss. Aug. 14, 2008); *Mackelprang*, 2007 WL 119149 at *2 ("Defendant . . . served a subpoena on MySpace.com . . . .").

38. *In re Skerry*, 2009 WL 1097326, at *1 ("Facebook sent an email in response [to a subpoena], indicating that it was creating a preservation order but that a formal subpoena was necessary before any documents would be produced.").

39. *Ledbetter*, 2009 WL 1067018, at *1-2.

40. *Id.*

> (2) a person or entity providing *remote computing service* to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . .[41]

The Act does provide exceptions for requests from an intended recipient of the communication, the "originator" of the communication, and law enforcement or governmental agencies if related to a criminal matter or a lawful wiretap.[42]

However, the statute does not authorize the "electronic communication service" or "remote computing service" to divulge such information pursuant to a civil subpoena.[43] Although the statute does not define "electronic communication service," courts have held that the Act prohibits web-based email providers, including Microsoft Mail, Google Mail, and Yahoo! Mail, from releasing the contents of a customer's email account pursuant to a civil subpoena.[44] In *J.T. Shannon Lumber Co. v. Gilco Lumber, Inc.*, the plaintiff subpoenaed the defendants' emails and account information directly from Microsoft, Google, and Yahoo!.[45] The defendants moved to quash the subpoenas.[46] The court held that because the exceptions to the Stored Communications Act "do not include [an exception for] a civil subpoena," the subpoenas were unenforceable.[47] Although the court did not state exactly why Google, Yahoo!, and Microsoft constituted either "electronic communication services" or "remote computing services," it did hold that the "statutory language is clear and unambiguous" and that "[t]he Act creates a zone of privacy that protects internet subscribers from having their personal information wrongfully used and disclosed by unauthorized private parties."[48]

Were a court to conclude that social networking sites, many of which contain embedded email and instant messaging programs, are akin to Google Mail or Yahoo! Mail and are thus within the definition of an "electronic communication service" or "remote computing service," then it is possible that Facebook, MySpace, and other social networking sites could take the position that they are prohibited from complying with a third-party civil subpoena requesting ESI relating to their customer's pages. Although the Act provides no definition for "electronic communication service," it does define a "remote computing service" as "the provision to the public of *computer storage* or *processing services* by

---

41. 18 U.S.C.A. §§ 2702(a)(1)-(2) (2000) (emphasis added).

42. *Id.* §§ 2702(b), 2703(a)-(d).

43. J.T. Shannon Lumber Co. v. Gilco Lumber, Inc., No. 2:07-CV-119, 2008 WL 3833216, at *1 (N.D. Miss. Aug. 14, 2008); *see also* 18 U.S.C. § 2702 (failing to list an exception for civil subpoenas).

44. *J.T. Shannon Lumber Co.*, 2008 WL 3833216 at *2.

45. *Id.* at *1.

46 *Id.*

47. *Id.*

48. *Id.* at *2. This is a remarkable opinion because it implicitly defines a party requesting information from a web-mail provider through a lawful civil subpoena as an "unauthorized" party.

means of an electronic communications system."[49] To the extent that Facebook and other social networking sites provide the public with a place to "store" personal information and to "process" the information they have stored through web-based software and programming, it would certainly seem that a social networking site is a "remote computing service."

To date, however, this author could find no case addressing the issue of whether social networking sites fall within the scope of the Stored Communications Act. To the contrary, the *Ledbetter* court held that a civil subpoena served on a social networking site was enforceable without ever addressing the Act.[50]

Moreover, Facebook pages and social networking sites contain much more than just Internet-based email. Thus, it is possible that the Stored Communication Act, which only protects *communications* from disclosure, may not prohibit these websites from divulging the other contents of someone's page, such as photos, the individual's "wall," his or her résumé, lists of contacts and "friends," or other data displayed on the page. Although the Act's protection has been held to include "instant messages,"[51] it has not been expanded to include social networking sites.[52]

Thus, the law is not settled, and currently no one can state with certainty whether a social networking site must divulge the contents of a customer's page pursuant to a valid civil subpoena served by someone other than the customer.

B. Civil Subpoenas from Individuals Seeking ESI from Their Own Social Networking Sites Are, However, Enforceable

What is clear is that civil subpoenas from individuals seeking ESI from their *own* social networking sites are indeed enforceable.[53] This is because the Stored Communications Act contains an unambiguous exception for communications requested by the originator or "with the lawful consent . . . of the customer or subscriber."[54]

---

49. 18 U.S.C.A. § 2711(2) (emphasis added).

50. Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *1-2 (D. Colo. Apr. 21, 2009).

51. Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1130 (C.D. Cal. 2006), *aff'd in part, rev'd in part on unrelated grounds*, 529 F.3d 892 (9th Cir. 2008), *cert. granted on unrelated grounds sub nom.* City of Ontario v. Quon, 130 S. Ct. 1011 (2009).

52. It is noteworthy that a bulletin board, a very basic form of chat room that bears some similarities to the Facebook "wall" has been held to be a "remote computing service." Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 442-43 (W.D. Tex. 1993). However, the *Steve Jackson Games* court did not directly address the issue whether the Stored Communications Act protects ESI other than "communications" from disclosure even if stored or created on a "remote computer service," because it held that the bulletin board in question was used to transmit e-mails and electronic communications. *Id.*

53. *See, e.g.*, Bass v. Miss Porter's School, No. 3:08cv1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009).

54. 18 U.S.C.A. § 2702(b)(3).

C. Governmental Entities Can Enforce Subpoenas Served on Social Networking Sites If They Relate to a Criminal Matter or Investigation

Even if a social networking site were held to be an "electronic storage service" and all of its contents were deemed "communications," there should also be no dispute that court orders and subpoenas requested by a governmental entity served upon a social networking site and related to criminal matters are enforceable.[55] Although most of the decisions discussing criminal subpoenas served on social networking sites do not discuss the Stored Communication Act, the Act allows "electronic communication services" and "remote computing services" to divulge information to the government about customers pursuant to a valid warrant or court order in a criminal case, but not a civil one.[56]

VI. SUGGESTIONS AND CONCLUSIONS

A. Until the Law Is Clear, Individuals and Businesses Should Take All Reasonable Steps to Preserve the Potentially Relevant Contents of Any Social Networking Pages for Which They Are Responsible

If parties believe that a current *or past* version of their Facebook or social networking pages may be relevant to foreseeable or ongoing civil litigation, then most judges will require them, as with any other relevant ESI, to preserve and produce the contents of those pages. However, because we update, view, and create information on our social networking pages over the Internet, our pages are stored primarily on the servers and storage devices hosted by the sites themselves. Therefore, there is no simply way to "preserve" and later produce something that is not under our control in the traditional sense.

However, until the law provides greater clarity, an individual who believes his Facebook page might be evidence in a foreseeable or ongoing lawsuit should:

- Send a formal written request (email should suffice) to the social networking site requesting a "preservation order."[57] Even if the site does not comply, you will have helped to protect yourself from spoliation claims.
- Print off pages from your Facebook page or take screen shots and save them.

---

55. *Id.* § 2703; *see also* United States v. Lemon, No. 08-246 (DSD/SRN), 2008 WL 4999235, at *3 (D. Minn. Nov. 18, 2008) (describing an FBI subpoena served on Google and Yahoo! seeking webmail that would otherwise be protected by the Stored Communications Act).

56. 18 U.S.C. § 2703(c)-(d).

57. *See In re* Skerry, No. C-09-80070 MISC CRB (EMC), 2009 WL 1097326, at *1 (N.D. Cal. Apr. 20, 2009) (stating that Facebook informed the petitioner that it was "creating a preservation order" to preserve his page's contents still saved on Facebook's system).

- Do your best to save or archive your social networking page on your own computer. Although it may not be possible to retain the entire page or its functionality, it may be possible to save important portions of your page and avoid any claims of spoliation.

For corporations that encourage employees to use Facebook or LinkedIn for business purposes, it is very likely that the employees' pages are business records and thus within the sea of ESI and documents that the company must preserve if relevant to a foreseeable lawsuit. In such a situation, if within the budget, the company should engage a computer forensics expert, who should be able to successfully archive the social networking pages as of the time of the litigation hold and thus avoid any claims that the company failed to discharge its duties to preserve and produce relevant social networking ESI in the lawsuit.

It is also very important for businesses that encourage their employees to use social networking sites to create and follow policies for updating these pages so that all versions are captured (and so employees do not share or disclose over Facebook, LinkedIn, or the like information that should be kept confidential).

Even if an individual or business makes all reasonable efforts to preserve the contents of social networking pages within their control, there still may be relevant ESI that is only controlled by the site itself. Although no court has addressed the issue—and despite the *Mackelprang* decision, which suggests in *dicta* that the account-holder, not the site, has the duty to preserve and produce the contents of his or her page[58]—it seems axiomatic that no court would hold individuals or businesses responsible for destroying ESI that was never in their control.

However, there may be occasions when the ESI that is only held by the site may be needed to resolve a dispute or provide evidence at trial. Information about who is viewing someone's social networking page, which other pages the individual has visited, and other metadata about the account-holder's activities and viewing patterns might only be kept by the social networking site itself.[59] In those cases, both the account-holders themselves and third parties seeking to discover this metadata should use subpoenas to request the information. Although the site may have some defenses based upon the Stored Communications Act if the subpoena requests information about another party, a subpoena is still the best way to recover this important evidence.

58. Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc., No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, at *8-9 (D. Nev. Jan. 9, 2007).

59. *See, e.g.*, Regard & Matzen, *supra* note 15.

B. The Courts Should Interpret the Federal Stored Communications Act, or the Legislature Should Amend the Act, to Allow Social Networking Sites to Divulge Information Pursuant to a Valid Civil Subpoena

In addition to these practical suggestions for practitioners and individuals faced with the current uncertainty in the law, either legislatures or the courts should determine whether social networking sites, like Facebook and LinkedIn, should be governed by the Stored Communications Act. Specifically, courts or legislatures should clarify whether these sites provide either "electronic communication services" or "remote computing services" and whether all of the contents of a social networking site, not just the embedded email and messaging functions, are "communications" within the scope of the Act. Until the law is clear, parties cannot adequately determine who is required to preserve and produce the relevant contents of social networking sites in civil litigation and from whom the parties should request the information, which is unquestionably ESI and discoverable if relevant.[60]

C. Social Networking Sites Should Be Required to Enact a Procedure and Create a Mechanism Through Which an Individual User Can Institute a Litigation Hold on His or Her Page and All Historical Versions of the Page Still Stored by the Social Networking Site

If the courts or legislatures decide that social networking sites are prohibited from disclosing the contents of a customer's page pursuant to a civil subpoena to anyone other than the customers themselves, these sites should be required to implement a system through which each account-holder can implement a litigation hold on (and request copies of) their social networking pages and any historical versions of those pages still in existence. To allow otherwise would make it impossible for an individual to comply with his or her duties to preserve and produce ESI, which some courts already assume are within their control.[61]

---

60. *See supra* Part II.

61. *See Mackelprang*, 2007 WL 119149, at *8 (stating that if the producing party failed to produce relevant ESI from her MySpace page, she could be sanctioned).

* * *