Spring 2014
Vol. 23, No. 3

pass it on

The newsletter of the American Bar Association's Government and Public Sector Lawyers Division

Discovery of Evidence Using Social Media:
Seven Tips for Government Lawyers

by Ted Hirt

Social media are an important means by which an organization communicates its mission and accomplishments.[1] Government agencies' presence on these media platforms is increasing.[2] Correspondingly, government employees, like everyone else, are increasingly communicating via social media.

A significant amount of potentially discoverable information now resides on Facebook, Twitter, and LinkedIn among other social media sites. To competently represent their clients, government lawyers need to understand their office's social media policy and stay current on issues involving discovery of social media in civil litigation.[3]

To illustrate some common social media discovery challenges, assume that a government employee has brought an employment discrimination and retaliation case against her agency. The plaintiff alleges that a supervisor not only denied her a promotion, but also made disparaging comments about her at the agency and outside the office.

Interviews of the supervisor and other employees in the work unit reveal that the plaintiff has made postings about the office, her career progress, and her colleagues on her own Facebook page. Agency counsel's discovery plan should consider whether and how to obtain information from social media for defense of the agency's decisions or other conduct, and to rebut the plaintiff's claims. Below are seven tips on how to address challenges raised in this type of social media discovery process.

Tip 1

Do not assume easy access to social media information. Access is not automatic, despite the breadth of discovery permitted under the Federal Rules of Civil Procedure and many state rules. Some courts have held that an employer may demand access to the plaintiff's social media site in situations where the employee has placed his or her emotional state at issue.[4] Consider if that applies in your case—does the employee assert that the employment decision or alleged retaliation caused her emotional suffering? If so, agency counsel may be able to convince the court that the inquiry is relevant.

Tip 2

Consider potential privacy objections. Agency counsel may encounter a threshold objection that the employee's social media postings are private, i.e., limited to a discrete set of people. But, if the court is provided some evidence that the request will yield relevant information, this argument may fail. The court will attempt to balance the parties' interests. Some courts have required the requesting party to make a threshold showing that publicly available information on the sites undermines the other party's claims. Marshal any information publicly available to support defense claims and/or an argument that the plaintiff has effectively waived privacy claims.[5] For example, assemble the employee's public social media posts about the incidents at issue or the effects of employment decisions on his or her emotional or career development.

AMERICAN BAR ASSOCIATION
Government and Public Sector Lawyers Division

Tip 3 **Subpoenas to the social media provider will likely fail.** Keep in mind that the employee is the only source for this social media information. While a party can obtain social media information by deposition notice or subpoena from the subscriber, access to the information by a subpoena to the social media provider is "off limits" because of the restrictions of the Stored Communications Act.[6]

Tip 4 **Avoid fishing expeditions.** Consider the temporal scope of the employee's case and the relevant period of the employment decisions. Social media discovery raises important issues of proportionality and burden. Presented with this potential resource, there may be a temptation to request all information that the employee has posted on her social media sites and, similarly, to request all postings by others in response to those postings. Sweeping requests for information may be rebuffed because a court may be sensitive to privacy concerns.[7] The judge also may conclude that an overly broad request is the kind of "fishing expedition" that is prohibited under the discovery rules. As one district court judge observed, the fact that the information "is in an electronic file as opposed to a file cabinet does not give the [party] the right to rummage through the entire file."[8]

Tip 5 **Be sure that the discovery request is focused.** The agency attorney should develop a targeted request and, if feasible, should accompany that request with a showing that there is reason to believe that relevant information is located on the employee's social media account. Also, keep in mind that if a large quantity of information is obtained, a correspondingly large amount of time will be needed to review the postings. Some of that time may be more effectively used on other discovery or case tasks.

Tip 6 **Investigate and preserve sources of relevant information at the agency.** The agency attorney must be aware of the possibility that sources of relevant information may be located on the agency's own website or social media sites, on the social media sites of other employees, or in other media. This raises important issues of information preservation. Agency staff must consider how to preserve information stored on the agency's servers that may be relevant to the case.[9] Agency staff should coordinate their efforts with the information technology and/or records management personnel to secure the information from inadvertent (automatic) or purposeful deletion.

Tip 7 **Be aware of ethical implications.** Social media discovery implicates several important ethics issues. First, the attorney must not advise the agency client to modify or delete postings or comments on a social media site—that will be considered the spoliation of relevant evidence and could lead to the imposition of sanctions by the court.[10] In at least one case, an attorney has been sanctioned by courts for that advice.[11]

Second, agency attorneys must avoid the temptation to create a social media account, or to use an intermediary to obtain information about the

Does your agency have a "Bring Your Own Device" (BYOD) policy?

Agency counsel must learn if such a policy exists and if the policy allows agency access to that stored information. The widespread use of mobile devices means that potentially relevant information is decentralized within the agency. Because employees use electronic devices for both official and personal communications, access to the information poses new challenges.

Member Editor
Pauline Weaver

Staff Editors
Katherine Mikkelson
Susan Kidd

Comments, letters to the editor and other suggestions
Editor, Government and Public Sector Lawyers Division
American Bar Association
1050 Connecticut Ave., NW, Suite 400
Washington, DC 20036
202-662-1020

E-mail
GPSLD@americanbar.org

Visit our homepage
www.governmentlawyer.org

Reprint requests must be made in writing to copyright@americanbar.org.

Editorial Statement
Pass It On provides a forum for the discussion of issues of special concern to government and public sector lawyers. *Pass It On* is edited by members of the Government and Public Sector Lawyers Division. Publishing and editorial decisions are based on the editors' judgment of the quality of the writing, the timeliness of the article, and the potential interest to the readers of *Pass It On*. The views in *Pass It On* are those of the authors and may not reflect the official policy of the American Bar Association or the Government and Public Sector Lawyers Division. No endorsement of the views should be inferred unless specifically identified as the official policy of the American Bar Association or the Government and Public Sector Lawyers Division.

AMERICAN BAR ASSOCIATION
Government and Public Sector Lawyers Division

opposing party or a witness outside the formal discovery procedures. That conduct may violate bar rules on contacts with represented persons.[12]

We can expect more developments in the law and technology of social media. Government lawyers should continue to educate themselves on these issues as agencies continue to use and seek access to social media sources.

Privacy is a central issue in "social media discovery." Government agencies collect a wide variety of information, much of it private or sensitive, from individuals, companies, and nonprofit groups. Agency employees have duties imposed by law, e.g., the federal Privacy Act, to safeguard such information.[13] The law is not settled as to an employee's privacy expectations related to electronic equipment owned by the government agency.[14]

Ted Hirt is a Washington, D.C. attorney who has written on e-discovery and related issues for the Division's publications. The views expressed are entirely his own.

Endnotes

1. An excellent source on social media issues is *The Sedona Conference® Primer on Social Media*, 14 Sedona Conf. J. 191 (Fall 2013).
2. *See* Lidsky, *Government Sponsored Social Media and Public Forum Doctrine: Perils and Pitfalls*, 19 The Public Lawyer 2, 3 (Summer 2011).
3. *See* Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 Rich J.L. & Tech. 12 (2013); Loop and Malyshev, *How to Manage a Company's Social Media Presence,* 24 No. 4 Intwell. Prop. & Tech. L.J. 3 (April 2013).
4. *See, e.g., Reid v. Ingerman Smith LLP*, 2012 WL 6720752, at *2 (E.D. N.Y. Dec. 27, 2012).
5. *See Jewell v. Aaron's Inc.*, 2013 WL 3770837 (N.D. Ga. July 19, 2013) (in a putative Fair Labor Standards Act class action, the court denied the company's motion for four years of Facebook postings by the 87 opt-in plaintiffs; the court considered the request excessive and not shown to lead to admissible evidence).
6. *See Crispin v. Christian Audiger, Inc.*, 717 F. Supp.2d 965, 975 (C.D. Cal. 2010); *FTC v. Netscape Comm. Corp.*, 196 F.R.D. 559 (N.D. Cal. 2000).
7. *Giacchetto v. Patchogue-Medford Union Free School Dist.*, 293 F.R.D. 112, 115 (E.D.N.Y. 2013) ("a plaintiff's entire social networking account is not necessarily relevant simply because he or she is seeking emotional distress damages").
8. *Howell v. Buckeye Ranch, Inc.*, 2012 WL 5265170 (S.D. Ohio Oct. 1, 2012).
9. See *Gatto v. United Airlines, Inc.*, 2013 WL 1285285, at *3 (D. N.J. March 25, 2013).
10. See *Gatto, supra*, 2013 WL 1285285, at *4 (rejecting plaintiff's assertion that he acted reasonably in deactivating his Facebook account after receiving notice from Facebook that the account has been accessed from an unauthorized IP address, insofar as the deactivation resulted in the deletion of relevant evidence and prejudice to defendants).
11. *See* Bennett, *Ethical Limitations on Informal Discovery of Social Media Information*, 36 Am. J. Trial Advoc. 473, 493 (2013).
12. *See* Bennett, *supra*, at 483-87.
13. *See* 5 U.S.C. § 552a.
14. *See City of Ontario v. Quon*, 560 U.S. 746, 130 S.Ct. 2619 (June 17, 2010). In *Quon*, the Court determined that a sheriff's department could inspect messages on employee pager devices as part of an audit of employee use of the department-owned devices. The Court remarked that a "reasonable employee would be aware that sound management principles" might require an audit - whether the pager w was being appropriately used. 130 S.Ct. at 2631.