THE SUFFOLK LAWYER
THE OFFICIAL PUBLICATION OF THE SUFFOLK COUNTY BAR ASSOCIATION
DEDICATED TO LEGAL EXCELLENCE SINCE 1908 www.scba.org Vol. 32, No. 7– March 2017

CYBER

E-Discovery of Social Media

By Victor Yannacone

This is part one of a series.

The 2017 presidential election campaign have made it perfectly clear that there can be no expectation of privacy with respect to social media. Social media has now replaced email as our primary means of electronic communications. Since 2009, there have been more social network users and more time spent on social media than email.

The total blurring of any distinctions between "personal" and "business" uses of social media platforms, accelerated by "Bring Your Own Device" (BYOD) policies that allows employees, particularly contract employees, to use their preferred mobile devices for work means that attorneys can no longer ignore their obligations under FRCP Rule 37 to become familiar with their clients' information systems and digital data — including all their social media.

At the intake interview, or shortly thereafter, attorneys must ask their clients for a list of all their personal social media accounts and other electronic repositories that may contain personal information. If it is not immediately forthcoming, they should decline to continue representing the client.


Victor Yannacone

E-Discovery rules apply to social media activity

Social media communications and online activity are "electronically stored information" (ESI). When the *Federal Rules of Civil Procedure* were amended in 2006 to include ESI, the term was "intended to be read expansively to include all current and future electronic storage mediums."[1]

Communications stored in the "cloud" or on a social networking site will be treated as discoverable ESI subject to the non-delegable duty to preserve relevant or potentially relevant information once litigation is pending or reasonably anticipated.

For the party filing the legal action, the litigation hold and "do not destroy" notice by the attorney should be triggered before the complaint is filed. "A duty to preserve evidence arises when there is knowledge of a potential claim."[2]

The standard for preservation is "reasonableness and proportionality." The proactive advice provided by FINRA to broker dealers in January 2010 says it most succinctly: "Every firm that intends to communicate, or permit its associated persons to communicate, through social media sites must first ensure that it can retain records of those communications…"

Screenshots of social media are not sufficient because social media files consist of more than just posts. They consist of related links, videos, embedded files, and metadata, all of which are part of the record. All original unaltered source files and any other data referenced or linked to the page are the best evidence of a particular post when captured in real-time. Social media content is updated, changed, or deleted on an ongoing basis. Failure to capture, record and preserve those changes may be considered evidence of spoliation and sanctions may be imposed.

There are some limits on e-Discovery of social media

Fortunately, courts have consistently refused to permit litigants to engage in social media fishing expeditions. The social media must contain relevant material. A demand for "all documents concerning, relating to, reflecting and/or regarding Plaintiff's utilization of social networking sites" should be rejected if there is no specificity to the requests and no effort to limit these requests to any relevant acts alleged in the action.

(Continued on page 26)

Demands for "any documents, postings, pictures, messages, or entries of any kind on social media within the covered period relating to claims by a party or their experts" are objectionable because they are not narrowly drawn and do not describe the categories of material sought.

Demands for any profiles, postings or messages from social media sites relating to any mental state of the plaintiff; third-party communications to the plaintiff that place her own communications in context; and any pictures of the plaintiff may be denied, unless a clear showing of relevancy is made. However, a demand for social networking communications of a party with any other party or potential witness in the litigation or that in any way pertain to the subject matter of the lawsuit will be approved.

It appears from the reported cases that the court will conduct a "traditional relevance analysis" whenever a demand for production of social media is challenged.

Preservation of social media — an ongoing challenge

Outside corporate firewalls and beyond the control of internal legal and IT teams, social media data is not only difficult to identify but difficult to preserve when litigation is reasonably foreseeable.

The problem is now moving from major litigation between corporate behemoths to personal injury actions and matrimonials. Defendants in personal injury actions and both parties in contested matrimonials are routinely requesting eDiscovery of social media.

Courts are increasingly willing to grant defense motions for an "adverse inference spoliation sanction" against parties for failing to preserve social media accounts provided the moving party can establish four factors: control, actual suppression or withholding of evidence, relevance, and foreseeability.

- Control is established by showing that a party had authority to modify the content of the account.
- Relevance is shown the way it always has since the Anglo-American system of adversary jurisprudence arose in America during the 17th century.
- Foreseeability is generally determined from the precision with which the demand for preservation was made and whether reasonable period of time has passed between service of a demand and the act of spoliation.

Controversies arise over determining whether actual suppression or withholding of evidence occurred. A clever but disingenuous and specious argument often raised is that the service provider is responsible for maintaining and preserving the account since the user of the account has no "administrator" privileges. This argument fails if the spoliation occurs after service of a proper litigation hold notice because the burden is on the party who generates the social media and maintains the account, not the service provider, to "preserve relevant evidence."

Attorneys representing litigants or clients who may become litigants must be proactive and the most effective action is a written memo advising the client to:

- Conduct a comprehensive data assessment to identify what social media information is held, where it's stored and how it's generated and used.
- Create a defensible comprehensive social media plan.
- Leverage available technology to collect each social media posting together with its metadata as it is posted or immediately thereafter.

The next column will address the practical, but ever present, issue of authenticating social media postings.

Note: Victor John Yannacone Jr. is an advocate, trial lawyer, and litigator practicing today in the manner of a British barrister by serving of counsel to attorneys and law firms locally and throughout the United States in complex matters. Mr. Yannacone has been continuously involved in computer science since the days of the first transistors in 1955 and actively involved in design, development, and management of relational databases. He pioneered in the development of environmental systems science and was a cofounder of the Environmental Defense Fund. Mr. Yannacone can be reached at (631) 475-0231, or vyannacone@yannalaw.com, and through his website https://yannalaw.com.

[1] Notes of the Advisory Committee to the 2006 Amendments to Rule 34.

[2] *Micron Tech., v. Rambus*, 255 F.R.D. 135 (D.Del.2009), aff'd 645 F.3d 1311 (Fed. Cir. 2011).