THE MEDIA GRAY ZONE: APPLICATIONS OF OPEN SOURCE INTELLIGENCE IN THE LEGAL FIELD

SPEAKER:
SKYE CHANCE COOLEY, Ph.D.

THURSDAY, JULY 27, 2017 • 3:45 - 4:45 PM

The Media Gray Zone: Communication Strategies for Lawyers in a Mediated World.

A PRESENTATION TO BATON ROUGE BAR ASSOCIATION

Goals today

Explanation of M3S technology

Detail the Background of the Research

Discuss SMA Deliverables related to the MGZ

Detail the Initial analysis and Findings

Discuss practical application for lawyers

Tools: Multi-media monitoring system (M3S) at Texas A&M:

- Allows harvesting, machine transcription, and machine translation of wide variety of media in four language streams:
  - Arabic
  - Farsi
  - Chinese
  - Russian
- Satellite Television: Al Arabiya, Al Jazeera, Rossiya 24, CCTV 4, Phoenix Infonews
- Web sites
  - Targeted websites triangulated by relationship to government

Defining the Gray Zone

The military definition of the Gray Zone occupies a center portion of a spectrum between the white space of peace and the blackness of war; an application of unconventional means to accomplish conventional warlike outcomes.

Our contribution to knowledge of the Gray Zone is based on the understanding that global media allows each citizen of every digitized nation to become both a weapon and a target of information and disinformation.

Conceptualizing the Media Gray Zone

From Berzins (2016)

The breaking of an enemy's resistance through technology, propaganda, and, ultimately, narrative control moves the battlefield lines to that of media power to influence, promote the inner decay of an opponent, engage in culture war and war of perception that takes place in human consciousness and in cyberspace, from a defined period to a permanent condition of natural life.

We define this mediated effort of ideological narrative control as the Media Gray Zone.

Conceptualizing the Media Gray Zone

Our definition of the MGZ mirrors and compliments that of traditional Gray Zone

The addition of the MGZ to the conceptualization of the Gray Zone adds needed clarity in the various applications of the GZ umbrella. It does so in four ways:

- First, it is a unique attempt to consider the GZ as sum of uniquely segmented parts.
  - The MGZ has its own distinctive spectrum of activity that build toward other GZ outcome predictors.
- Second, the MGZ allows for insight into the action of foreign actors in relation to others and relation to themselves within GZ spaces toward narrative bridges.
- Third, the MGZ allows us to more concretely assess how media messages move across populations and global media.
- Fourth, we believe our approach will inspire others to segment out GZ spaces towards better overall predictors.

Conceptualizing the Media Gray Zone

The spectrum of operation for the Media Gray Zone focuses on media conversations ranging from an inactive white space dealing with conversations on policy and diplomacy with ideological similar other, to a fully active black space discussing perspectives on actual ground conflicts with ideologically different other.

Those conversations straddling the line between to two extremes of the spectrum, we deem as the Media Gray Zone. A space of disinformation, fake news, manipulative narratives, and context creation with a focused outcome of accomplishing the management of public thought for both domestic and foreign audiences on matters related to the larger geo-political goals of the state.

Conceptualizing the Media Gray Zone

Therefore mediated gray zone conflict is, in its most simplistic terms, a battle over identities, problem and solution labeling, narrative crafting and dissemination to challenge, suppress, and/or support narratives of other actors.

Outcomes in the MGZ:

- Represent changes in the information environment favorable to the country employing specific narratives in the global media-scape.

Victory in the MGZ

- Represents the ability to suppress information from other in favor of one's own position, toward the securement and/or furthering of the ideological foundations of the state.

Each actor in the MGZ does this with both foreign and domestic audiences.

The MGZ Spectrum of Space

White Space

- Stable world order with actors in ideological agreement built upon shared values, norms, and identities affirmed in common principles and institutions. Media provides a continuous confirmation and socialization for members.

Gray Space

- Attempts at reconfiguring or challenging of values, norms, and identities with multiple actors in ideological disagreement across the global media-scape. Media serves to redefine norms, values, and identities of citizens toward the global order. Process involves questioning actions of others, the credibility of others, the intentions of others, and suggesting revision to the current order.

Black Space

- Actor no longer seeks placement in current global order, but seeks to dismantle it. Media serves to propagandize military actions, overt psychological warfare, and bolster state material and military support.

Legal ramifications

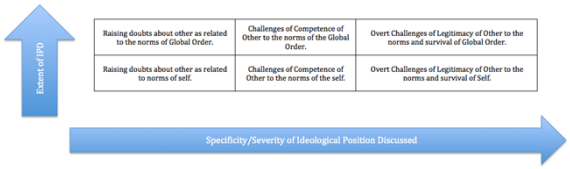
Narrative battles that take place in the MGZ are not confined to battles between state actors. These narrative conflicts take place between our own domestic political parties, between media and grassroots activists, between corporations, and most certainly in legal battles and the presentation of legal issues to the public.

For attorneys, battles in the MGZ are as real and as consequential as they are for the DoD. One conceptualization is that of the trial.

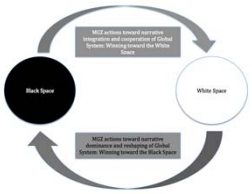
- Think of the White space as an area of non-conflict, normative
- Black space is trial itself
- The MGZ is what happens in the middle, the battle for narrative positioning
  - Lawyer advertising
  - Pretrial communication
  - Establishing the important issues of attention in the trial

The MGZ Spectrum of Space

Within the Media Gray Zone, Gray space, specific actions and challenges take place upon a gradient of more contentious actions, creating increasing divergence toward the Black space.



The MGZ Spectrum of Space



Winning in the MGZ

Four primary strategies for victory:

- Presentation of self and others in global order and relational links/divisions
- Penetration of the information environment of other and defense of one's own (information flow control)
- Revision narratives (constructive or destructive)
- Relaying grand vision of self in global order to foreign and domestic audiences.

Actors pursuing revisionist system narratives can do so in concert with other nations to reset the global order peacefully, and thus move a united system, under a revised global system toward the white space. However, when cooperation of narratives breaks down between individual actors, or with their linked partners, **there is acceleration to the black space**.

Applications for Legal Practice

Once again, this spectrum is not limited to military applications, but can serve as a measure of escalation toward a white space event or dominant narrative framework.

Depending on your aims, this can serve as a measure of successfully winning in either direction toward white or black spaces. Better said, either preventing narrative shift, or as accomplishing it in the MGZ and would serve the legal field with an assessment of efforts to alter narratives concerning their client, scope of the trial, or a number of other pre-trial applications.

Application of MGZ: World Watches the U.S. Election

Our current global order, while linked economically, has significantly competing narratives concerning foundational approaches to governance and stability.

The United States and the West drive forth media narratives concerning the common cores of democracy and the value of progressive social liberalism toward an equitable existence for all of humanity.

Increasingly, Russia, Iran, and China drive narratives that outline versions authoritarianism as models for creating stability, security from external threats, and in fostering more morally sound ways of existence.

While not all of the involved actors are in direct cooperation, the MGZ is currently in an information battle to reshape the narrative on the global order and the roles of the actors involved there within that pushes very near to the black space.

Overall project context

US Presidential election matters not just to US citizens, but around the world.

US had outsized impact on global economy and politics

Serves as an indicator of future US policy

Serves as a way to reflect/comment on US political practices and values

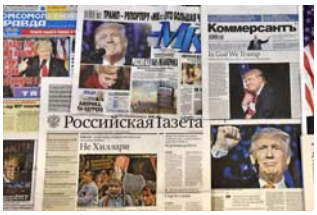
- "Democracy"

Russia Views the US Election

Skye Cooley-Oklahoma State University

Ethan Stokes-University of Alabama

In the interest of time, I will only present the Russian related findings of this case study.



MGZ Context

The outcome of the 2016 U.S. presidential election for Russia was one of tremendous importance.

- Pressures from Western sanctions for Russia's involvement in Ukraine and Crimea
- Military escalations, tensions, and fragile agreements between the US and Russia over Syria
- The refugee crisis facing Europe over conflicts throughout North Africa and the Middle East
- Rising troop movements along the Baltic borders saw U.S. Russian relations deteriorate during the Obama administration

The Russian regime saw the U.S. and Western spread of global democracy as a threat to its sphere of influence and to the legitimacy of its rule.

- Viewed a continuation of the policies of the Obama administration as less than optimal
- Repeatedly vowed to work with whichever candidate who won the U.S. election

Method

Inductive Narrative Analysis focused on MGZ spectrum related to:

- Legitimacy, the democratic process and its desirability, coverage of the candidates, metaphors on the election and democracy, and overall themes presented through the narratives.

Data Collection:

- Pulled from 3 time periods (1 week before, the week of, & 1 week after) during the 2016 U.S. presidential election campaign:
  1) **Republican & Democratic National Conventions** (Data Pull: 7/11/2016 – 8/4/2016)
  - RNC: 7/18/2016-7/21/2016
  - DNC: 7/25/2016-7/28/2016
  2) **First Presidential Debate** (Data Pull: 9/19/2016 – 10/3/2016)
  - First Presidential Debate: 9/26/2016
  3) **Election Day** (Data Pull: 11/1/2016 – 11/15/2016)
  - Election Day: 11/8/2016

4 Search Terms:

- "Donald Trump," "Hillary Clinton," "Republican Party," and "Democratic Party."

Method

Table 1: Russian News Story Frequencies by Data Pull & Search Term

Data Pull	"Donald Trump"	"Hillary Clinton"	"Rep. Party"	"Dem. Party"	Total (*N*):
RNC/DNC	918	749	541	595	**2,803**
First Debate	384	309	206	450	**1,349**
Election Day	910	614	373	510	**2,407**
Total (*N*):	**2,212**	**1,672**	**1,120**	**1,555**	**6,559**

Scope:

- Initially pulled 6,000 Russian web and broadcast news stories
- Stratified random sample of 523 Russian news stories
- Inter-coder reliability (*n* = 200 stories)

The presentation will break up the coverage by: **Pro-Government**, **stated Neutral**, and **stated Oppositional** news sources.

Findings: Pro-Government (*n* = 211)

A Hypocritical, Failing US System of Globalism Overtaken by Trump; The Hope for Failure.

Clinton: 33 (15%) stories were directly critical of Clinton, 3 (1%) stories were in praise of Clinton, and two of those were reports on President Obama's words concerning her ability to lead.
- Presented as corrupt, illegitimate, a liar, a manipulator, and an enemy of Russia.

Trump: 26 (12%) stories were directly critical of Trump, while 12 (6%) were in direct praise of Trump.
- Presented as cautious optimism. Viewed Trump as potentially favorable to Russia, but also as a wild card.

The State of American Democracy: 50 (23%) stories questioned the legitimacy of U.S. democracy and of its candidates. While 39 (18%) stories were critical of the U.S. the election process itself.
- Framed in a desperate light, with only a handful of stories showing U.S. democracy positively.

RNC/DNC:
- Presented the Republican Party as fractured over Trump, and Democrats as mired in scandals, corruption, and investigations.

First Debate:
- Presented the first debate as a spectacle of non-stop arguing and mudslinging entertainment for enormous ratings.

Election Day:
- Presented Trump's victory as hopeful for Russia both in the policies he will pursue and what his victory represents about the U.S.

Findings: Neutral (*n* = 156)

The Russian, Trump, & Wikileaks Triumvirate: The Rise of American Authoritarianism.

Clinton: 10 (6%) stories were directly critical of Clinton, while 2 (1%) were in direct praise of Clinton. Most of the coverage of Clinton was neutral and concerned poll numbers, lead changes, and similarities to President Obama.

- Presented Clinton as under attack from Russian officials and cyber-hacking, Wikileaks, and Donald Trump.

Trump: 44 (28%) of the stories were directly critical of Trump, while 4 (2%) were in direct praise of Trump.

- Presented Trump as likely to make the lives of Russians, Americans, and others worse as he increasingly mirrors Putin.

The State of American Democracy: 43 (28%) stories questioned the legitimacy of United States democracy and of its candidates. While 47 (30%) stories were critical of the U.S. the election process itself.

- A corrupted failure of elite, and capitalist, driven globalism now facing the same style of authoritarianism as Russia.

RNC/DNC:

- Claimed the U.S. increasingly looks like the Russian system, neither being democratic, and both using TV as a propaganda tool against its people.

First Debate:

- Presented the first debate as a spectacle of entertainment, and the U.S. election as a scandalous system that is more of a fundraising and entertainment vehicle for American society than one representative of democracy.

Election Day:

- Presented U.S. democracy approaching authoritarianism, with no one to blame but itself.

Findings: Oppositional (*n* = 155)

The Game of Thrones and Confusion.

Clinton: 12 (8%) stories were directly critical of Clinton, while 7 (5%) stories were in praise of Clinton.

- An assumption of certainty in Clinton's victory presented throughout, and as an extremely flawed candidate.

Trump: 32 (20%) of the stories were directly critical of Trump, while 14 (9%) were in direct praise of Trump.

- Presented as both a toxic poison to the GOP and U.S. democracy, and yet still a legitimate representation of the populism.

The State of American Democracy: 23 (14%) stories questioned the legitimacy of U.S. democracy and of its candidates. 13 (8%) stories showed U.S. democracy as a legitimate voice of the American people. 9 (6%) stories were critical of the U.S. the election process itself.

RNC/DNC:

- Presented the U.S. as a polarized, disrupted state of political unrest with the comical presence of Donald Trump and the scandals unfolding within the Clinton campaign.

First Debate:

- Claims U.S. politics has become populist beer-drinking entertainment, and is representative of its people.

Election Day:

- Much coverage following Trump's victory was more intensely focused on the state of the global order, showing NATO, the UK, the Ukraine, and a host of others working to understand Trump's positions and worrying over potential outcomes.

Common Narratives from Sources

Common Narratives:

- The entertainment spectator sport that American democracy has become
- The strength of populist movements as a result of globalization
- The sincere flaws of the candidates being put forward
- The end of American Exceptionalism

Pro-government sources presented the rise of Trump as beneficial to Russia.

Neutral sources showed the rise of Trump as the end of the American democratic experiment.

Oppositional sources do their best to show a system in shock, but still able to represent its people.

The illegitimacy of the office of the U.S. presidency and of our entire process is notable as well in pro-government and neutral sources.

Common Narratives Related to MGZ

Our findings, from Russian coverage of the US election highlight MGZ activity and narrative creation surrounding four issues relating to the United States.

- Accusations of Russian manipulation of the U.S. election
- The imposed U.S. led sanctions against Russia
- The Syrian civil war
- The collapse of Western democracy.

Manipulation of the U.S. Election

Russia is presented as a victim of accusations, innocent of any wrong-doing, and willing to cooperate.

Clinton is presented as creating a Red Scare in order to win the election.

Trump shown as a supporter of Russian positions and used to bolster Russian claims of innocence.

While there are repeated challenges to the competency of Clinton, Trump is covered in a light of cautious optimism toward finding common ground and re-establishing a more trustful relationship between the U.S. and Russia.

Trump's ultimate victory in the election made coverage of the issue of accusations against Russia in the election shift to a more cooperative tone. **Russian officials are quoted as willing to participate with the United States toward a more cooperative relationship and world order. It is left up to the United States and its leaders to do so.**

Imposed US led Sanctions

Russia is presented as being able to determine its own borders and destiny, not to be bullied by globalist bent on suppression.

Trump's comments used to bolster territorial claims of Crimea and Putin's leadership style.

Concern for war, and the risk of war by globalist to win an election.

Sanctions a punishment mechanism of ruling globalist who wish to promote fear of Russia for their own benefit.

NATO a threat to Russia and in disarray after Trump victory

Imposed US led Sanctions

The specter of possible war over globalist policies specifically targeting Russia in order to destabilize the regime is an alarming challenge to the global order, Russian media shows at least one party in the United States political system as literally willing to risk war in order to prevent nations such as Russia from deciding their own territorial boundaries and knowing how best to deal with their neighboring nations.

Russian media constantly refers to NATO as an external threat used by globalists to prevent Russia from being an autonomous nation.

Trump's victory is the only factor that lightens the tone of these discussions, and that is with a resignation that very little would be worse for Russia than a Clinton victory.

The Syrian Civil War

Russian media presented the Syrian civil war as a micro-representative of the differing macro-foreign policy agendas between the West (particularly the United States) and itself.

Presentation of self showed Russia as a reasonable peace-broker concerned with stabilizing the Middle East and defeating terrorism.

The Obama administration is shown in a light of past failures in the Middle East, Libya most pointedly. The administration is presented as concerned more with pushing a global, capitalist, agenda over that of true concern for Middle Eastern stability. Furthermore, mentions of Obama as rushing to quickly resolve the Syrian civil war in order to end his legacy as that of a peacemaker highlight the lack of long-term thought the administration gives to the region.

The Syrian Civil War

The presentation of the Syrian war shows the U.S. as having ill thought through foreign policies, for reasons more concerned with self than with the actual region, and such policies must change in order to accomplish peace.

The United States is presented as an actor that must begin working with other nations to accomplish the goals related to global stability, instead of pursuing its own selfish concerns.

There is hope for future cooperation and genuine concern for a potential election of Hillary Clinton, who is presented as a potential escalator of conflict.

The Collapse of Western Democracy

The presentation of the U.S. election process as showcasing the collapse of Western democracy is by far the most powerful and most present occurring topic discussed throughout the entire dataset, and it is the culmination of various narratives in the MGZ by Russia to show that the global order needs to change and is already in the process of the change toward new leadership.

Russian media presents the U.S. election as a highlight to the over-extension of globalism, that Western democracies are elite run systems that have lost touch with their own citizens and on the verge of collapse.

The corruption and lack of qualifications of leadership of the candidates is covered at great length. Clinton in particular is presented as undermining Bernie Sanders, in collusion with U.S. media, scandal riddled (FBI, emails, and foundation scandals) and willing to do and say anything in order to win the election.

The Collapse of Western Democracy

Russian media presents Russia as a nation willing to watch the U.S. system, and all of Western democracy, collapse on itself. While U.S. system failure might result in global conflict, financial market collapses, or further disruptions to global stability in vulnerable parts of the world, the Western model is shown as something that has overreach so far that it is unlikely to be able to save itself.

Russia is shown as a sane alternative to Western democracy.

Russian media uses the U.S. election process to make a case for its system of governance to be a more sensible, and cooperative, model toward a new global order, in replacement of Western globalism and all of its failures.

Overall MGZ Presentation

The results of these findings across the dataset show **Russia as overtly challenging the legitimacy of a U.S. led global order, and as seeking to redefine, through narratives, its position in the global order.**

Russia is shown as a respected, sensible, and cooperative nation that is tired of being bullied by an elitist U.S. system that is willing to spread globalism by the sword in order to accomplish its own objectives…even when those objectives mean undermining U.S. citizens.

It is a call for a change of the global order guard, and Russia is actively shown as a nation ready to work with others who would also like to see a change to the system…further, Russian media claim the change is happening without any direct action by itself or others.

Winning Toward the Black Space

The U.S. system and all of Western democracy are collapsing under the weight of their own greed and over expansion.

Russia is simply positioning itself to fill the void. Ultimately, it is a concerted information campaign to win toward the black space of the MGZ.

And from our data, Russia is not the only actor involved in an attempt to win toward the black space.

Consequences

We can clearly see that US as leader of a global order is being challenged as legitimate.

US soft-power and Western democracy have taken a serious hit through the US election, and media have used the coverage to legitimize alternative forms of government and alternative world order. Putin is able to justify both his leadership and his anti-Western policies by driving these narratives to his domestic audience. Inoculating himself from criticism and justifying his fears of Western aggression.

These calls lack uniformity, but uniformity would certainly pose a serious threat toward actual conflict if they continue unchecked.

Recommendation

Better narrative control on US democratic process (stop providing ammunition)

Clearer explanations of foreign policy that is in continuity with democratic principles

Exploiting cooperative narratives of others; forcing exchange

Develop strategies of narrative cooperation to win toward the white space and retain/evolve the global order.

Involves other SMA teams to link sub-analyses to MGZ predictors, and better empirical approaches toward MGZ strategies when manifest.

Applying Open Source to Legal Practice

Narrative Monitoring and Control

- *How are you monitoring competitors in the gray space of legal competition*
  - *You have a social media presence*
  - *How are potential clients viewing situations*
- *Complex/ public litigation*
  - *What is the community sentiment toward the primary issues with which your practice deals*
  - *What are the primary narratives surrounding the issues with which your practice deals*
  - *Who controls those narratives, and in what communities*

Applying Open Source to Legal Practice

Beyond Narrative Control

-Practices are currently using open source applications for:

- Event recreation
- Witness intelligence
- Network Analysis

Summing Up

Open Source technologies like the M3S, used with a communication focus can serve to:

- Recognize threats to and Protect important narratives to your practice
- Recognize weaknesses and Attack important narratives to your competitors (and their clients)
- Give important analytic tools to better inform you about your clients & witnesses and those across the aisle.
- Help reconstruct events and offer clearer reconstruction of those events to jurors and witnesses

The principle applications are the same for you as they are for the government as these technologies provide dramatic strategic advantages for those who possess and utilize them.

The Media Gray Zone:
Applications of Open Source Intelligence in the Legal Field

Presented by:
Dr. Skye Cooley

Table of Contents

AUTHENTICATION

419 Md. 343
19 A.3d 415

Antoine Levar GRIFFIN
v.
STATE of Maryland.

Court of Appeals of Maryland.

April 28, 2011.

[419 Md. 346] In this case, we are tasked with determining the appropriate way to authenticate, for evidential purposes, electronically stored information printed from a social

[19 A.3d 417]

networking website,[1] in particular, MySpace.[2]

Antoine Levar Griffin, Petitioner, seeks reversal of his convictions in the Circuit Court for Cecil County, contending that the trial judge abused his discretion in admitting, without proper authentication, what the State alleged were several pages printed from Griffin's girlfriend's MySpace profile. [3] The Court of Special Appeals determined that the trial judge did not abuse his discretion, *Griffin v. State,* 192 Md.App. 518, 995 A.2d 791 (2010), and we granted Griffin's Petition for Writ of Certiorari, 415 Md. 607, 4 A.3d 512 (2010), to consider the two questions, which we have rephrased:

1. Did the trial court err in admitting a page printed from a MySpace profile alleged to be that of Petitioner's girlfriend? [4]

[419 Md. 347] 2. Did the trial court err in allowing the prosecutor to define reasonable doubt incorrectly over defense objection, including saying "it means this, do you have a good reason to believe that somebody other than Mr. Griffin was the person that shot Darvell Guest ... I'm not asking you whether you can speculate and create some construct of hypothetical possibilities that would have somebody else be the shooter.... I'm asking you the question, do you have right now any reason, any rational reason to believe that somebody other than he was the shooter or gunman?" [5]

The State presented a conditional cross-petition, which we also granted, in which one question was posed:

1. Is Griffin's challenge to the probative value of the evidence preserved for appellate review? [6]

[19 A.3d 418]

We shall hold that the pages allegedly printed from Griffin's girlfriend's MySpace profile were not properly authenticated pursuant to Maryland Rule 5–901,[7] and shall, therefore, reverse[419 Md. 348] the judgment of the Court of Special Appeals and remand the case for a new trial.

Griffin was charged in numerous counts with the shooting death, on April 24, 2005, of Darvell Guest at Ferrari's Bar in Perryville, in Cecil County. During his trial, the State sought to introduce Griffin's girlfriend's, Jessica Barber's, MySpace profile to demonstrate that, prior to trial, Ms. Barber had allegedly threatened another witness called by the State. The printed pages contained a MySpace profile in the name of "Sistasouljah," describing a 23 year-old female from Port Deposit, listing her birthday as "10/02/1983" and containing a photograph of an embracing couple. The printed pages also contained the following blurb:

FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!

When Ms. Barber had taken the stand after being called by the State, she was not questioned about the pages allegedly printed from her MySpace profile.

Instead, the State attempted to authenticate the pages, as belonging to Ms. Barber, through the testimony of Sergeant John Cook, the lead investigator in the case. Defense counsel objected to the admission of the pages allegedly printed from Ms. Barber's MySpace profile, because the State could not sufficiently establish a "connection" between the profile and posting and Ms. Barber, and substantively, the State could not say with any certainty that the purported "threat" had any [419 Md. 349] impact on the witness's testimony; the latter argument is not before us.

Defense counsel was permitted to voir dire Sergeant Cook, outside of the presence of the jury, as follows:

[Defense Counsel]: How do you know that this is her [MySpace] page?....

[Sergeant Cook]: Through the photograph of her and Boozy on the front, through the reference to Boozy, [ ] the reference [to] the children, and [ ] her birth date indicated on the form.

[Defense Counsel]: How do you know she sent it?

[Sergeant Cook]: I can't say that.

[The Court]: I failed—I am sorry. I misrepresented. I failed to realize there is a photograph there. It's in the block

[19 A.3d 419]

that says "Sistasouljah," and then there's a photograph of a person that looks like Jessica Barber to me.

[Defense Counsel]: When was it sent?

[Sergeant Cook]: That is a MySpace page. That wasn't particularly sent. That is on the web, and it's accessible to whoever views MySpace. It is open to the public.

[Defense Counsel]: I understand that. When did it get posted?

[Sergeant Cook]: The print date on the form, printed on 12/05/06.

[The Court]: You can tell by looking at it because that's when he went to it.

[Defense Counsel]: So that would have been after the first trial. So how could that possibly affect [the witness]? He said it was before the first trial.

[The Court]: On its face, there is no way that you can conclude that on its face this establishes anything in regard to [the witness]. What it's being offered for, as I understand it, is corroboration, consistency that she's making a statement in a public forum, "snitches get stitches." And I guess the argument is going to be made that that's consistent with what [the witness] said, that she threatened him.

[419 Md. 350] [Assistant State's Attorney]: That's correct.

[The Court]: It's weak. I mean, there is no question it's weak, but that's what it is offered for.

The trial judge, thereafter, indicated that he would permit Sergeant Cook to testify in support of authentication of the redacted portion of the pages printed from MySpace, containing the photograph "of a person that looks like Jessica Barber" and the Petitioner, allegedly known as "Boozy," adjacent to a description of the woman as a 23 year-old from Port Deposit, and the blurb, stating "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"

In lieu of Sergeant Cook's testimony, while maintaining his objection to the admissibility of the redacted MySpace page, defense counsel agreed to the following stipulation:

If asked, Sergeant Cook would testify that he went onto the Internet to the website known as MySpace.... [F]rom that site he downloaded some information of a posting that someone had put there.

That posting contains a photograph which the witness would say he recognizes as a photograph of Jessica ... Barber, who testified, ... that she is the defendant's live-in fiance; and that it also contains a date of birth, to wit October 2nd, 1983, which the witness would testify is the date of birth that Jessica Barber gave as her date of birth.

When the exhibit, the download, comes to you, you are going to see that it has a great—that most of its content has been redacted; that is, blacked out. That's because some of it, in my judgment, might tend to be inflammatory without proving anything one way or the other. There

is one portion of it that will not be redacted when it comes to you, and this is the only portion of it which you should consider. And you certainly should not speculate as to what any of the redacted portions may be.

The portion that will not be redacted says, just remember snitches get stitches. You will see that. The phrase is, just remember snitches get stitches.... And ... the witness [419 Md. 351] would testify that the date it was retrieved was ... December 5, 2006.

Whether the MySpace printout represents that which it purports to be, not only a MySpace profile created by Ms. Barber,

[19 A.3d 420]

but also upon which she had posted, "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!," is the issue before us.

With respect to social networking websites in general, we have already had occasion, in *Independent Newspapers, Inc. v. Brodie,* 407 Md. 415, 424 n. 3, 966 A.2d 432, 438 n. 3 (2009), to describe those sites as "sophisticated tools of communication where the user voluntarily provides information that the user wants to share with others." [8] A number of social networking websites, such as MySpace, enable members "to create online 'profiles,' which are individual web pages on which members [can] post photographs, videos, and information about their lives and interests." *Doe v. MySpace, Inc.,* 474 F.Supp.2d 843, 845 (W.D.Tex.2007).

Anyone can create a MySpace profile at no cost, as long as that person has an email address and claims to be over the age of fourteen:

MySpace users create profiles by filling out questionnaire-like web forms. Users are then able to connect their profiles to those of other users and thereby form communities. MySpace profiles contain several informational sections, known as "blurbs." These include two standard blurbs: "About Me" and "Who I'd Like to Meet." Users may supplement those blurbs with additional sections about their interests, general additional details, and other personal information. MySpace profiles also incorporate several [419 Md. 352] multimedia features. For instance, users may post photos, music, videos, and web logs to their pages.

Richard M. Guo, *Stranger Danger and the Online Social Network,* 23 Berkeley Tech. L.J. 617, 621 (2008) (footnotes omitted). After a profile is established, the user may invite others to access her profile, as a "friend," who if the user accepts the befriending, can access her profile pages without further ado:

Users establish virtual communities by linking their profiles in a process known as "friending" or "connecting." One user requests to add another as a friend, and the recipient may either accept or reject the invitation. If the recipient accepts, the profiles are linked and the connected members are generally able to view one another's online content without restriction. The network created by the linking process allows a user to chat with friends, display support for particular causes, "join interest groups dedicated to virtually any topic," and otherwise "hang

out."

Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking,* 93 Marq. L.Rev. 1495, 1499–1500 (2009–2010) (footnotes omitted). Although a social networking site generally requires a unique username and password for the user to both establish a profile and access it, posting on the site by those that befriend the user does not. *See* Samantha L. Miller, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet,* 97 Ky. L.J. 541, 544 (2008–2009); Eric Danowitz, *MySpace Invasion: Privacy Rights, Libel, and Liability,* 28 J. Juv. L. 30, 37 (2007).

[19 A.3d 421]

The identity of who generated the profile may be confounding, because "a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate." Petrashek, 93 Marq. L.Rev. at 1499 n. 16. The concern arises because anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password:

[419 Md. 353] Although it may seem that, as creators of our own online social networking profiles, we are able to construct our own online persona, this is not always the case. There is no law that prevents someone from establishing a fake account under another person's name, so long as the purpose for doing so is not to deceive others and gain some advantage. Moreover, fragments of information, either crafted under our authority or fabricated by others, are available by performing a Google search ... forever. Thus, online social networking poses two threats: that information may be (1) available because of one's own role as the creator of the content, or (2) generated by a third party, whether or not it is accurate.

David Hector Montes, *Living Our Lives Online: The Privacy Implications of Online Social Networking,* Journal of Law and Policy for the Information Society, Spring 2009, at 507, 508. For instance, in one circumstance, Sophos, a Boston-based Internet security company, created a profile for a toy frog named "Freddi Staur," and nearly 200 Facebook [9] users [419 Md. 354] chose to add the frog as a "friend." Miller, 97 Ky. L.J. at 542.[10]

The possibility for user abuse also exists on MySpace, as illustrated by *United States v. Drew*, 259 F.R.D. 449 (D.C.D.Cal.2009), in which Lori Drew, a mother, was prosecuted under the Computer Fraud and

[19 A.3d 422]

Abuse Act, 18 U.S.C. § 1030, for creating a MySpace profile for a fictitious 16 year-old male named "Josh Evans." Drew had contacted a former friend of her daughter's, Megan Meier, through the MySpace network, using the Josh Evans screen name or pseudonym, and began to "flirt with her over a number of days." *Id.* at 452. Drew then had "Josh" inform Megan that he no longer "liked her" and that "the world would be a better place without her in it," after which

Megan killed herself. *Id*. Thus, the relative ease with which anyone can create fictional personas or gain unauthorized access to another user's profile, with deleterious consequences, is the *Drew* lesson.

The potential for fabricating or tampering with electronically stored information on a social networking site, thus poses significant challenges from the standpoint of authentication of printouts of the site, as in the present case. Authentication, nevertheless, is generally governed by Maryland Rule 5–901, which provides:

(a) **General provision.** The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

[419 Md. 355] Potential methods of authentication are illustrated in Rule 5–901(b). The most germane to the present inquiry are Rules 5–901(b)(1) and 5–901(b)(4), which state:

(b) **Illustrations.** By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this Rule:

(1) Testimony of witness with knowledge. Testimony of a witness with knowledge that the offered evidence is what it is claimed to be.[11]

(4) Circumstantial evidence. Circumstantial evidence, such as appearance, contents, substance, internal patterns, location, or other distinctive characteristics, that the offered evidence is what it is claimed to be.

We and our colleagues on the Court of Special Appeals have had the opportunity to apply the tenets of Rule 5–901(b)(4) to a toxicology report, *State v. Bryant,* 361 Md. 420, 761 A.2d 925 (2000), to recordings from 911 emergency calls, *Clark v. State,* 188 Md.App. 110, 981 A.2d 666 (2009), and to text messages received on the victim's cellular phone, *Dickens v. State,* 175 Md.App. 231, 927 A.2d 32 (2007), but neither we nor our appellate brethren heretofore has considered the Rule's application to authenticate pages printed from a social networking site.

Rather, we turn for assistance to the discussion in *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D.Md.2007), wherein Maryland's own Magistrate Judge Paul W. [419 Md. 356] Grimm, a recognized authority on evidentiary issues concerning electronic evidence, outlined issues regarding authentication of electronically stored information, in e-mail, websites, digital photographs, computer-generated documents,

[19 A.3d 423]

and internet postings, etc. with respect to Rule 901 of the Federal Rules of Evidence:

(a) **GENERAL PROVISION.** The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

(b) **ILLUSTRATIONS.** By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

(1) *Testimony of Witness With Knowledge.* Testimony that a matter is what it is claimed to be.

* * *

(4) *Distinctive Characteristics and the Like.* Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

Regarding Rule 901(a), Judge Grimm iterated in *Lorraine* that the "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims," to insure trustworthiness. *Id.* at 541–42. Judge Grimm recognized that authenticating electronically stored information presents a myriad of concerns because "technology changes so rapidly" and is "often new to many judges." *Id.* at 544. Moreover, the "complexity" or "novelty" of electronically stored information, with its potential for manipulation, requires greater scrutiny of "the foundational requirements" than letters or other paper records, to bolster reliability. *Id.* at 543–44, quoting Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 900.06[3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997).

In the present case, Griffin argues that the State did not appropriately, for evidentiary purposes, authenticate the [419 Md. 357] pages allegedly printed from Jessica Barber's MySpace profile, because the State failed to offer any extrinsic evidence describing MySpace, as well as indicating how Sergeant Cook obtained the pages in question and adequately linking both the profile and the "snitches get stitches" posting to Ms. Barber. The State counters that the photograph, personal information, and references to freeing "Boozy" were sufficient to enable the finder of fact to believe that the pages printed from MySpace were indeed Ms. Barber's.

We agree with Griffin and disagree with the State regarding whether the trial judge abused his discretion in admitting the MySpace profile as appropriately authenticated, with Jessica Barber as its creator and user, as well as the author of the "snitches get stitches" posting, based upon the inadequate foundation laid. We differ from our colleagues on the Court of Special Appeals, who gave short shrift to the concern that "someone other than the alleged author may have accessed the account and posted the message in question." *Griffin*, 192 Md.App. at 542, 995 A.2d at 805. While the intermediate appellate court determined that the pages allegedly printed from Ms. Barber's MySpace profile contained sufficient indicia of reliability, because the printout "featured a photograph of Ms. Barber and [Petitioner] in an embrace," and also contained the "user's birth date and identified her boyfriend as 'Boozy,' " the court failed to acknowledge the possibility or likelihood that another user could have created the profile in issue or authored the "snitches get stitches" posting. *Id.* at 543, 995 A.2d at 806.

We agree with Griffin that the trial judge abused his discretion in admitting

[19 A.3d 424]

the MySpace evidence pursuant to Rule 5–901(b)(4), because the picture of Ms. Barber, coupled with her birth date and location, were not sufficient "distinctive characteristics" on a MySpace profile to authenticate its printout, given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the "snitches get stitches" comment. The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion [419 Md. 358] that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the "snitches get stitches" language.[12]

In so holding, we recognize that other courts, called upon to consider authentication of electronically stored information on social networking sites, have suggested greater scrutiny because of the heightened possibility for manipulation by other than the true user or poster. In *Commonwealth v. Williams*, 456 Mass. 857, 926 N.E.2d 1162 (2010), the Supreme Judicial Court of Massachusetts considered the admission, over the defendant's objection, of instant messages a witness had received "at her account at MySpace." *Id.* at 1171. In the case, the defendant was convicted of the shooting death of Izaah Tucker, as well as other offenses. The witness, Ashlei Noyes, [419 Md. 359] testified that she had spent the evening of the murder socializing with the defendant and that he had been carrying a handgun. She further testified that the defendant's brother had contacted her "four times on her MySpace account between February 9, 2007, and February 12, 2007," urging her "not to testify or to claim a lack of memory regarding the events of the night of the murder." *Id.* at 1172. At trial, Noyes testified that the defendant's brother, Jesse Williams, had a picture of himself on his MySpace account and that his MySpace screen name or pseudonym was "doit4it." She testified that she had received the messages from Williams, and the document printed from her MySpace account indicated that the messages were in fact sent by a user with the screen name

[19 A.3d 425]

"doit4it," depicting a picture of Williams. *Id.*

The Supreme Judicial Court of Massachusetts determined that there was an inadequate foundation laid to authenticate the MySpace messages, because the State failed to offer any evidence regarding who had access to the MySpace page and whether another author, other than Williams, could have virtually-penned the messages:

Although it appears that the sender of the messages was using Williams's MySpace Web "page," there is no testimony (from Noyes or another) regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc. Analogizing a MySpace [message] to a telephone call, a witness's testimony that he or she has received an incoming call from a person claiming to be "A," without more, is insufficient evidence to admit

the call as a conversation with "A." Here, while the foundational testimony established that the messages were sent by someone with access to Williams's MySpace Web page, it did not identify the person who actually sent the communication. Nor was there expert testimony that no one other than Williams could communicate from that Web page. Testimony regarding the contents of the messages should not have been admitted.

Id. at 1172–73 (citations omitted). The court emphasized that the State failed to demonstrate a sufficient connection between [419 Md. 360] the messages printed from Williams's alleged MySpace account and Williams himself, with reference, for example, to Williams's use of an exclusive username and password to which only he had access. The court determined that the error in admitting the improperly authenticated MySpace messages "did not create a substantial likelihood of a miscarriage of justice," however, and, therefore, did not reverse Williams's conviction, because Noyes's testimony was significantly overshadowed "by the testimony of two witnesses to the murder who identified Williams as the shooter." *Id.* at 1173.

Similarly, in *People v. Lenihan*, 30 Misc.3d 289, 911 N.Y.S.2d 588 (N.Y.Sup.Ct.2010), Lenihan challenged his second degree murder conviction because he was not permitted to cross-examine two witnesses called by the State on the basis of photographs his mother had printed from MySpace, allegedly depicting the witnesses and the victim making hand gestures and wearing clothing that suggested an affiliation with the "Crips" gang. The trial judge precluded Lenihan from confronting the witnesses with the MySpace photographs, reasoning that "[i]n light of the ability to 'photo shop,' edit photographs on the computer," Lenihan could not adequately authenticate the photographs. *Id.* at 592.

In *United States v. Jackson*, 208 F.3d 633 (7th Cir.2000), Jackson was charged with mail and wire fraud and obstruction of justice after making false claims of racial harassment against the United Parcel Service in connection with an elaborate scheme in which she sent packages containing racial epithets to herself and to several prominent African–Americans purportedly from "racist elements" within UPS. *Id.* at 635. At trial, Jackson sought to introduce website postings from "the Euro–American Student Union and Storm Front," in which the white supremacist groups gloated about Jackson's case and took credit for the UPS mailings. *Id.* at 637. The court determined that the trial judge was justified in excluding the evidence because it lacked an appropriate foundation, namely that Jackson had failed to show that the web postings by the white

[19 A.3d 426]

supremacist groups who took responsibility for [419 Md. 361] the racist mailings "actually were posted by the groups, as opposed to being slipped onto the groups' websites by Jackson herself, who was a skilled computer user." *Id.* at 638.

The State refers us, however, to *In the Interest of F.P.*, 878 A.2d 91 (Pa.Super.Ct.2005), in which the Pennsylvania intermediate appellate court considered whether instant messages were properly authenticated pursuant to Pennsylvania Rule of Evidence 901(b)(4), providing that a document may be authenticated by distinctive characteristics or circumstantial evidence. In the

case, involving an assault, the victim, Z.G., testified that the defendant had attacked him because he believed that Z.G. had stolen a DVD from him. The hearing judge, over defendant's objection, admitted instant messages from a user with the screen name "Icp4Life30" to and between "WHITEBOY Z 404." *Id.* at 94. Z.G. testified that his screen name was "WHITEBOY Z 404" and that he had printed the instant messages from his computer. In the transcript of the instant messages, moreover, Z.G. asked "who is this," and the defendant replied, using his first name. Throughout the transcripts, the defendant threatened Z.G. with physical violence because Z.G. "stole off [him]." *Id.* On appeal, the court determined that the instant messages were properly authenticated through the testimony of Z.G. and also because "Icp4Life30" had referred to himself by first name, repeatedly accused Z.G. of stealing from him, and referenced the fact that Z.G. had told high school administrators about the threats, such that the instant messages contained distinctive characteristics and content linking them to the defendant. *In the Interest of F.P.* is unpersuasive in the context of a social networking site, because the authentication of instant messages by the recipient who identifies his own "distinctive characteristics" and his having received the messages, is distinguishable from the authentication of a profile and posting printed from MySpace, by one who is neither a creator nor user of the specific profile. [13]

[419 Md. 362] Similarly, the State relies upon an unreported opinion, *State v. Bell*, 2009 WL 1395857, 2009 Ohio App. LEXIS 2112 (Ohio Ct.App.2009), in which the defendant, convicted of multiple counts of child molestation, asserted that the trial judge

[19 A.3d 427]

improperly admitted "online conversations and email messages" on MySpace, purportedly involving Bell and one of his victims. The defendant argued that the messages were not properly authenticated, because his laptop "was turned on after it was seized," which he asserted altered hundreds of files on the hard drive. *Id.* at *4, 2009 Ohio App. LEXIS 2112 at *10. The appellate court rejected that argument because defense counsel had expressly approved the admission of the MySpace emails and messages. Griffin, in the present case, however, explicitly objected to the authenticity of the MySpace printout.

In the case sub judice, the MySpace printout was used to show that Ms. Barber had threatened a key witness, who the State had characterized as "probably the most important witness in this case;" the State highlighted the importance of [419 Md. 363] the "snitches get stitches" posting during closing argument, as follows:

Sergeant Cook told you that he went online and went to a website called MySpace and found a posting that had been placed there by the defendant's girlfriend, Jessica Barber, recognized her picture, able to match up the date of birth on the posting with her date of birth, and the posting included these words, "Free Boozy. Just remember, snitches get stitches. You know who you are."

In addition, during rebuttal argument, the State again referenced the pages printed from MySpace, asserting that Ms. Barber had employed MySpace as a tool of intimidation against a witness for the State. It is clear, then, that the MySpace printout was a key component of the

State's case; the error in the admission of its printout requires reversal.

In so doing, we should not be heard to suggest that printouts from social networking sites should never be admitted. Possible avenues to explore to properly authenticate a profile or posting printed from a social networking site, will, in all probability, continue to develop as the efforts to evidentially utilize information from the sites increases. *See, e.g.,* Katherine Minotti, Comment, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession,* 60 S.C.L.Rev. 1057 (2009). A number of authentication opportunities come to mind, however.

The first, and perhaps most obvious method would be to ask the purported creator if she indeed created the profile and also if she added the posting in question, i.e. "[t]estimony of a witness with knowledge that the offered evidence is what it is claimed to be." Rule 5–901(b)(1). The second option may be to search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question. One commentator, who serves as Managing Director and Deputy General Counsel[419 Md. 364] of Stroz Friedberg, [14] a computer forensics firm, notes that, "[s]ince a user unwittingly leaves an evidentiary trail on her computer simply by using it, her computer will provide evidence of her web usage." Seth P. Berman, et al., *Web 2. 0:*

[19 A.3d 428]

What's Evidence Between "Friends"?, Boston Bar J., Jan.-Feb.2009, at 5, 7.

A third method may be to obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it. This method was apparently successfully employed to authenticate a MySpace site in *People v. Clevenstine,* 68 A.D.3d 1448, 891 N.Y.S.2d 511 (2009). In the case, Richard Clevenstine was convicted of raping two teenage girls and challenged his convictions by asserting that the computer disk admitted into evidence, containing instant messages between him and the victims, sent via MySpace, was not properly authenticated. Specifically, Clevenstine argued that "someone else accessed his MySpace account and sent messages under his username." *Id.* at 514. The Supreme Court of New York, Appellate Division, agreed with the trial judge that the MySpace messages were properly authenticated, because both victims testified that they had engaged in instant messaging conversations about sexual activities with Clevenstine through MySpace. In addition, an investigator from the computer crime unit of the State Police testified that "he had retrieved such conversations from the hard drive of the computer used by the victims." *Id.* Finally, the prosecution was able to attribute the messages to Clevenstine, because a legal compliance officer for MySpace explained at trial that "the messages on the computer disk had been exchanged by users of accounts created by [Clevenstine] and the victims." *Id.* The [419 Md. 365] court concluded that such testimony provided ample authentication linking the MySpace messages in question to Clevenstine himself.[15]

JUDGMENT OF THE COURT OF SPECIAL APPEALS REVERSED. CASE REMANDED TO THAT COURT WITH INSTRUCTIONS TO REVERSE THE JUDGMENT OF THE CIRCUIT COURT FOR CECIL COUNTY AND REMAND THE CASE TO THE CIRCUIT COURT FOR A NEW TRIAL. COSTS IN THIS COURT AND IN THE COURT OF SPECIAL APPEALS TO BE PAID BY CECIL COUNTY.

See also Parker v State, 85 A.3d 682 (Del. 2014); Grant Guillot, *Evidentiary Implications of Social Media: An Examination of the Admissibility of Facebook, MySpace and Twitter Postings in Louisiana Courts*, 61 La. B.J. 338 (2014) .

PRIVACY

162 So.3d 146

Maria F. Leon NUCCI and Henry Leon, her husband, Petitioners
v.
TARGET CORPORATION, American Cleaning Contracting, Inc., and First Choice Building Maintenance, Inc., Respondents.

District Court of Appeal of Florida, Fourth District.

Jan. 7, 2015.

Opinion

GROSS, J.

In a personal injury case, Maria Nucci petitions for certiorari relief to quash a December 12, 2013 order compelling discovery of photographs from her Facebook account. The photographs sought were reasonably calculated to lead to the discovery of admissible evidence and Nucci's privacy interest in them was minimal, if any. Because the discovery order did not amount to a departure from the essential requirements of law, we deny the petition.

In her personal injury lawsuit, Nucci claimed that on February 4, 2010, she slipped and fell on a foreign substance on the floor of a Target store. In the complaint, she alleged the following:

- Suffered bodily injury
- Experienced pain from the injury
- Incurred medical, hospital, and nursing expenses, suffered physical handicap

• Suffered emotional pain and suffering

• Lost earnings

• Lost the ability to earn money

• Lost or suffered a diminution of ability to enjoy her life

• Suffered aggravation of preexisting injuries

• Suffered permanent or continuing injuries

• Will continue to suffer the losses and impairment in the future

Target took Nucci's deposition on September 4, 2013. Before the deposition, Target's lawyer viewed Nucci's Facebook profile and saw that it contained 1,285 photographs. At the deposition, Nucci objected to disclosing her Facebook photographs. Target's lawyer examined Nucci's Facebook profile two days after the deposition and saw that it listed only 1,249 photographs. On September 9, 2013, Target moved to compel inspection of Nucci's Facebook profile. Target wrote to Nucci and asked that she not destroy further information posted on her social media websites. Target argued that it was entitled to view the profile because Nucci's

[162 So.3d 149]

lawsuit put her physical and mental condition at issue.

Nucci's response to the motion explained that, since its creation, her Facebook page had been on a privacy setting that prevented the general public from having access to her account. She claimed that she had a reasonable expectation of privacy regarding her Facebook information and that Target's access would invade that privacy right. In addition, Nucci argued that Target's motion was an overbroad fishing expedition.

On October 17, 2013, the trial court conducted a hearing on Target's motion to compel. At the hearing, Target showed the court photographs from a surveillance video in which Nucci could be seen walking with two purses on her shoulders or carrying two jugs of water. Again, Target argued that because Nucci had put her physical condition at question, the relevancy of the Facebook photographs outweighed Nucci's right to privacy. It also argued that there was no constitutional right to privacy in photographs posted on Facebook. The circuit court denied Target's motion to compel, in part because the request was “vague, overly broad and unduly burdensome.”

Target responded to the court's ruling by filing narrower, more focused discovery requests. Target served Nucci with a set of Electronic Media Interrogatories, with four questions. It also served a Request for Production of Electronic Media, requesting nine items. In response to the interrogatories, Nucci objected on the grounds of (1) privacy; (2) items not readily accessible; and (3) relevance.

As to the Request for Production, Nucci raised the same three objections and additionally argued that the request was (4) overbroad; (5) brought solely to harass; (6) "over[ly] burdensome;" (7) "unduly burdensome"; and (8) unduly vague. Nucci raised only these general claims and no objections specifically directed at any particular photograph.

Target moved that the trial court disallow Nucci's objections. At a hearing on the motion, Target conceded that its request for production should be limited to photographs depicting Nucci. After a hearing on the motion, the trial court granted Target's motion in part and denied it in part. On December 12, 2013, the trial court compelled answers to the following interrogatories:

> 1. Identify all social/professional networking websites that Plaintiff is registered with currently (such as Facebook, MySpace, LinkedIn, Meetup.com, MyLife, etc.)
>
> 2. Please list the number and service carrier associated with each cellular telephone used by the Plaintiff and/or registered in the Plaintiff's name (this includes all numbers registered to and/or used by the Plaintiff under a "family plan" or similar service) at the time of loss and currently.

The order also compelled production of the following items:

> 1. For each social networking account listed in response to the interrogatories, please ***provide copies or screenshots of all photographs associated with that account during the two (2) years prior to the date of loss.***
>
> 2. For each social networking account listed in the interrogatories, provide ***copies or screenshots of all photographs associated with that account from the date of loss to present.***
>
> 3. For each cell phone listed in the interrogatories, please provide ***copies or screenshots of all photographs***

[162 So.3d 150]

> ***associated with that account during the two years prior to the date of loss.***
>
> 4. For each cellular phone listed in response to the interrogatories, please provide ***copies or screenshots of all photographs associated with that account from the date of loss to present.***
>
> 5. For each cellular phone listed in the interrogatories, please provide ***copies of any documentation outlining what calls were made or received on the date of loss.***

Nucci argues that the December 12 order departs from the essential requirements of the law because it constitutes an invasion of privacy.[1] Citing to *Salvato v. Miley*, No. 5:12–CV–635–Oc–

10PRI, 2013 WL 2712206 (M.D.Fla. June 11, 2013), which involved a request for e-mails and text messages, she contends that "the mere hope" that the discovery yields relevant evidence is not enough to warrant production. She also argues that the traditional rules of relevancy still apply to a request for social media materials. Nucci additionally asserts that her activation of privacy settings demonstrates an invocation of federal law. *See Ehling v. Monmouth–Ocean Hosp. Serv. Corp.*, 961 F.Supp.2d 659, 665 (D.N.J.2013). Relying upon *Ehling,* Nucci argues that her private Facebook posts were covered by the Federal Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 –2712, and were not therefore discoverable. We note that Nucci objected below to *all* disclosure; she did not attempt to limit disclosure of the photographs by establishing discrete guidelines. *See Reid v. Ingerman Smith LLP*, No. CV 2012–0307(ILG)(MDG), 2012 WL 6720752, at *2 (E.D.N.Y. Dec. 27, 2012) ; *E.E.O.C. v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 436 (S.D.Ind.2010).

In its response, Target points out, as it did below, that surveillance videos show Nucci carrying heavy bags, jugs of water, and doing other physical acts, suggesting that her claim of serious personal injury is suspect.

Target suggests that the material ordered is relevant to Nucci's claim of injury in that it allows a comparison of her current physical condition and limitations to her physical condition and quality of life before the date of the slip and fall. In its response to this Court, Target concedes that the order is limited to photographs depicting Nucci from the two years before the date of the incident to the present. It argues that the trial court did not grant unfettered access because it did not compel the production of passwords to her social networking accounts.

As to material injury or harm, Target points out that Nucci has not claimed that production of any particular photograph or other identifiable material will cause her damage or embarrassment. Citing to *Davenport v. State Farm Mutual Automobile Insurance Co.,* No. 3:11–cv–632–J–JBT, 2012 WL 555759 (M.D.Fla. Feb. 21, 2012), Target contends that the content of social networking sites is not privileged or protected by the right to privacy. It notes that Facebook's terms and conditions explain that, regardless of a user's intentions, the material contained in a post could be disseminated by Facebook at its discretion or under court order.

Finally, Target argues that in the context of a civil lawsuit, Florida courts can compel a party to release relevant records

[162 So.3d 151]

from social networking sites without implicating or violating the SCA.

Discussion

This case stands at the intersection of a litigant's privacy interests in social media postings and the broad discovery allowed in Florida in a civil case. Consideration of four factors leads to the conclusion that Nucci's petition for certiorari should be denied. First, certiorari relief is available in only a narrow class of cases and this case does not meet the stringent requirements for

certiorari relief. Second, the scope of discovery in civil cases is broad and discovery rulings by trial courts are reviewed under an abuse of discretion standard. Third, the information sought—photographs of Nucci posted on Nucci's social media sites—is highly relevant. Fourth, Nucci has but a limited privacy interest, if any, in pictures posted on her social networking sites.

Nucci's petition challenges only the discovery of photographs from social networking sites, such as Facebook. Thus, the order compelling the answers to interrogatories and production pertaining to a cellular phone are not at issue. Similarly, our ruling in this case covers neither communications other than photographs exchanged through electronic means nor access to other types of information contained on social networking sites.

Legal Standard for Certiorari

Certiorari is not available to review every erroneous discovery ruling. To be entitled to certiorari, the petitioner must establish three elements: " '(1) a departure from the essential requirements of the law, (2) resulting in material injury for the remainder of the case (3) that cannot be corrected on postjudgment appeal.' " *Williams v. Oken,* 62 So.3d 1129, 1132 (Fla.2011) (quoting *Reeves v. Fleetwood Homes of Fla., Inc.,* 889 So.2d 812, 822 (Fla.2004)). The last two elements, often referred to as "irreparable harm," are jurisdictional. If a petition fails to make a threshold showing of irreparable harm, this Court will dismiss the petition. *Bared & Co., Inc. v. McGuire,* 670 So.2d 153, 157 (Fla. 4th DCA 1996).

Overbreadth of discovery alone is not a basis for certiorari jurisdiction. *Bd. of Trs. of Internal Improvement Trust Fund v. Am. Educ. Enters., LLC,* 99 So.3d 450, 456 (Fla.2012). Similarly, mere irrelevance is not enough to justify certiorari relief. Certiorari may be granted from a discovery order where a party "affirmatively establishes" that the private information at issue is not relevant to any issue in the litigation and is not reasonably calculated to lead to admissible evidence. *Id.* at 457 (quoting *Allstate Ins. Co. v. Langston,* 655 So.2d 91, 95 (Fla.1995)); *see also Berkeley v. Eisen,* 699 So.2d 789 (Fla. 4th DCA 1997) (granting certiorari relief to protect privacy rights of non-parties to litigation). "The concept of relevancy has a much wider application in the discovery context than in the context of admissible evidence at trial." *Bd. of Trs.,* 99 So.3d at 458.

Certiorari relief is discretionary, but this Court should exercise this discretion only where the party has shown that " 'there has been a violation of clearly established principle of law resulting in a miscarriage of justice.' " *Williams,* 62 So.3d at 1133 (quoting *Haines City Cmty. Dev. v. Heggs,* 658 So.2d 523, 527 (Fla.1995)). The error must be serious to merit certiorari relief. Even where a departure from the essential requirements of law is shown, this Court may still deny the petition as certiorari relief is discretionary. *Id.*

[162 So.3d 152]

The Broad Scope of Discovery

A "part[y] may obtain discovery regarding any matter, not privileged, that is relevant to the

subject matter of the pending action, whether it relates to the claim or defense of the party seeking discovery or the claim or defense of any other party." Fla. R. Civ. P. 1.280(b)(1). "It is not ground for objection that the information sought will be inadmissible at the trial *if the information sought appears reasonably calculated to lead to the discovery of admissible evidence." Id.* (emphasis added). Florida Rule of Civil Procedure 1.350(a) includes electronically stored information within the scope of discovery.[2] An outer limit of discovery is that " 'litigants are not entitled to *carte blanche* discovery of irrelevant material.' " *Life Care Ctrs. of Am. v. Reese*, 948 So.2d 830, 832 (Fla. 5th DCA 2007) (quoting *Tanchel v. Shoemaker*, 928 So.2d 440, 442 (Fla. 5th DCA 2006)). Because the permissible scope of discovery is so broad, a "trial court is given wide discretion in dealing with discovery matters, and unless there is a clear abuse of that discretion, the appellate court will not disturb the trial court's order." *Alvarez v. Cooper Tire & Rubber Co.*, 75 So.3d 789, 793 (Fla. 4th DCA 2011) (direct appeal of discovery issue). It is because of this wide discretion accorded to trial judges that it is difficult to establish certiorari jurisdiction of discovery orders.

In a personal injury case where the plaintiff is seeking intangible damages, the fact-finder is required to examine the quality of the plaintiff's life before and after the accident to determine the extent of the loss. From testimony alone, it is often difficult for the fact-finder to grasp what a plaintiff's life was like prior to an accident. It would take a great novelist, a Tolstoy, a Dickens, or a Hemingway, to use words to summarize the totality of a prior life. If a photograph is worth a thousand words, there is no better portrayal of what an individual's life was like than those photographs the individual has chosen to share through social media before the occurrence of an accident causing injury. Such photographs are the equivalent of a "day in the life" slide show produced by the plaintiff before the existence of any motive to manipulate reality. The photographs sought here are thus powerfully relevant to the damage issues in the lawsuit. The relevance of the photographs is enhanced, because the post-accident surveillance videos of Nucci suggest that her injury claims are suspect and that she may not be an accurate reporter of her pre-accident life or of the quality of her life since then. The production order is not overly broad under the circumstances, as it is limited to the two years prior to the incident up to the present; the photographs sought are easily accessed and exist in electronic form, so compliance with the order is not onerous.

The Right of Privacy

To curtail the broad scope of discovery allowed in civil litigation, Nucci asserts a right of privacy. However, the

[162 So.3d 153]

relevance of the photographs overwhelms Nucci's minimal privacy interest in them.

The Florida Constitution expressly protects an individual's right to privacy. *See* Art. I, § 23, Fla. Const. ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."). This right is broader than the right to privacy implied in the Federal Constitution. *Berkeley*, 699 So.2d at 790. The right to

privacy in the Florida Constitution "ensures that individuals are able 'to determine for themselves when, how and to what extent information about them is communicated to others.' " *Shaktman v. State,* 553 So.2d 148, 150 (Fla.1989) (quoting A. Westin, *Privacy and Freedom* 7 (1967)).

Before the right to privacy attaches, there must exist a legitimate expectation of privacy. *Winfield v. Div. of Pari–Mutuel Wagering, Dep't of Bus. Regulation,* 477 So.2d 544, 547 (Fla.1985). Once a legitimate expectation of privacy is shown, the burden is on the party seeking disclosure to show the invasion is warranted by a compelling interest and that the least intrusive means are used. *Id.* In the civil discovery context, courts must engage in a balancing test, weighing the need for the discovery against the privacy interests. *Rasmussen v. S. Fla. Blood Serv., Inc.,* 500 So.2d 533, 535 (Fla.1987). If the person raising the privacy bar establishes the existence of a legitimate expectation of privacy, the party seeking to obtain the private information has the burden of establishing need sufficient to outweigh the privacy interest. *Berkeley,* 699 So.2d at 791–92.

In a thoughtful opinion, a Palm Beach County circuit judge has summarized the nature of social networking sites as follows:

> Social networking sites, such as Facebook, are free websites where an individual creates a "profile" which functions as a personal web page and may include, at the user's discretion, numerous photos and a vast array of personal information including age, employment, education, religious and political views and various recreational interests. *Trail v. Lesko,* [No. GD–10–017249,] 2012 WL 2864004 (Pa.Com.Pl. July 5, 2012). Once a user joins a social networking site, he or she can use the site to search for "friends" and create linkages to others based on similar interests. Kelly Ann Bub, Comment, *Privacy's Role in the Discovery of Social Networking Site Information,* 64 SMU L.Rev. 1433, 1435 (2011).
>
> Through the use of these sites, "users can share a variety of materials with friends or acquaintances of their choosing, including tasteless jokes, updates on their love lives, poignant reminiscences, business successes, petty complaints, party photographs, news about their children, or anything else they choose to disclose." Bruce E. Boyden, Comment, *Oversharing: Facebook Discovery and the Unbearable Sameness of Internet Law,* 65 Ark. L.Rev. 39, 42 (2012). As a result, social networking sites can provide a "treasure trove" of information in litigation. Christopher B. Hopkins, *Discovery of Facebook Contents in Florida Cases,* 31 No. 2 Trial Advoc. Q. 14 (2012).

Levine v. Culligan of Fla., Inc., Case No. 50–2011–CA–010339–XXXXMB, 2013 WL 1100404, at *2–*3 (Fla. 15th Cir.Ct. Jan. 29, 2013).

We agree with those cases concluding that, generally, the photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings

that the user may have established. *See Davenport v. State Farm Mut. Auto. Ins. Co.*, No. 3:11–cv–632–J–JBT, 2012 WL 555759, at *1 (M.D.Fla. Feb. 21, 2012) ; *see also Patterson v. Turner Constr. Co.*, 88 A.D.3d 617, 931 N.Y.S.2d 311, 312 (N.Y.App.2011) (holding that the "postings on plaintiff's online Facebook account, if relevant, are not shielded from discovery merely because plaintiff used the service's privacy settings to restrict access"). Such posted photographs are unlike medical records or communications with one's attorney, where disclosure is confined to narrow, confidential relationships. Facebook itself does not guarantee privacy. *Romano v. Steelcase, Inc.*, 30 Misc.3d 426, 907 N.Y.S.2d 650, 656 (N.Y.Sup.Ct.2010). By creating a Facebook account, a user acknowledges that her personal information would be shared with others. *Id.* at 657. "Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist." *Id.*

Because "information that an individual shares through social networking web-sites like Facebook may be copied and disseminated by another," the expectation that such information is private, in the traditional sense of the word, is not a reasonable one. *Beswick v. N.W. Med. Ctr., Inc.*, No. 07–020592 CACE(03), 2011 WL 7005038 (Fla. 17th Cir.Ct. Nov. 3, 2011). As one federal judge has observed,

> Even had plaintiff used privacy settings that allowed only her "friends" on Facebook to see postings, she "had no justifiable expectation that h[er] 'friends' would keep h[er] profile private...." *U.S. v. Meregildo*, 2012 WL 3264501, at *2 (S.D.N.Y.2012). In fact, "the wider h[er] circle of 'friends,' the more likely [her] posts would be viewed by someone [s]he never expected to see them." *Id.* Thus, as the Second Circuit has recognized, legitimate expectations of privacy may be lower in e-mails or other Internet transmissions. *U.S. v. Lifshitz*, 369 F.3d 173, 190 (2d Cir.2004) (contrasting privacy expectation of e-mail with greater expectation of privacy of materials located on a person's computer).

Reid v. Ingerman Smith LLP, No. CV2012–0307(ILG)(MDG), 2012 WL 6720752, at *2 (E.D.N.Y. Dec. 27, 2012) ; *see also Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387, 388 (E.D.Mich.2012) (holding that "material posted on a 'private' Facebook page, that is accessible to a selected group of recipients but not available for viewing by the general public, is generally not privileged, nor is it protected by common law or civil law notions of privacy"); *Mailhoit v. Home Depot U.S.A., Inc.*, 285 F.R.D. 566, 570 (C.D.Cal.2012) (indicating that social networking site content is neither privileged nor protected, but recognizing that party requesting discovery must make a threshold showing that such discovery is reasonably calculated to lead to admissible evidence).

We distinguish this case from *Root v. Balfour Beatty Construction, LLC*, 132 So.3d 867 (Fla. 2d DCA 2014). That case involved a claim filed by a mother on behalf of her three-year-old son who was struck by a vehicle. Unlike this case, where the trial court ordered the production of photographs from the plaintiff's Facebook account, the court in *Balfour* ordered the production of a much broader swath of Facebook material without any temporal limitation—postings,

statuses, photos, “likes,” or videos—that relate to the mother's relationships with all of her children, not just the three year old, and with “other family members, boyfriends, husbands, and/or significant others, both prior to, and following the accident.” *Id.* at 869. The second district determined that “social media evidence is discoverable,” but held that the ordered discovery was “overbroad” and compelled “the production

[162 So.3d 155]

of personal information ... not relevant to” the mother's claims. *Id.* at 868, 870. The court found that this was the type of “carte blanche” irrelevant discovery the Florida Supreme Court has sought to guard against. *Id.* at 870 ; *Langston,* 655 So.2d at 95 (“[W]e do not believe that a litigant is entitled *carte blanche* to irrelevant discovery.”) The discovery ordered in this case is narrower in scope and, as set forth above, is calculated to lead to evidence that is admissible in court.

Finally, we reject the claim that the Stored Communications Act, 18 U.S.C. §§ 2701 –2712, has any application to this case. Generally, the “SCA prevents ‘providers' of communication services from divulging private communications to certain entities and/or individuals.” *Quon v. Arch Wireless Operating Co., Inc.,* 529 F.3d 892, 900 (9th Cir.2008), *rev'd on other grounds by City of Ontario, Cal. v. Quon,* 560 U.S. 746, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010) (citation omitted). The act does not apply to individuals who use the communications services provided. *See, e.g., Flagg v. City of Detroit,* 252 F.R.D. 346, 349 (E.D.Mich.2008) (ruling that the SCA does not preclude civil discovery of a party's electronically stored communications which remain within the party's control even if they are maintained by a non-party service provider).

Finding no departure from the essential requirements of law, we deny the petition for certiorari.

STEVENSON and GERBER, JJ., concur.

Notes:

[1] The petition challenges the order to produce content from social networking sites. The petition does not challenge that portion of the orders below pertaining to a cellular telephone.

[2] Rule 1.350(a) states:

> Any party may request any other party (1) to produce and permit the party making the request, or someone acting in the requesting party's behalf, to inspect and copy any designated documents, *including electronically stored information,* writings, drawings, graphs, charts, photographs, phono-records, and other data compilations from which information can be obtained, translated, if necessary, by the party to whom the request is directed through detection devices into reasonably usable form, that constitute or contain matters within the scope of rule 1.280(b) and that are in the possession, custody, or control of the party to whom the request is

directed....

(Emphasis added).

---

18 F.Supp.3d 1346

Karen PALMA, et al., Plaintiffs,
v.
METRO PCS WIRELESS, INC., Defendant.

United States District Court, M.D. Florida, Tampa Division.

Signed April 29, 2014

Motion denied.

ORDER

MARK A. PIZZO, United States Magistrate Judge.

Defendant's motion to compel (doc. 204) and Plaintiffs' response (doc. 220) are before the Court. The District Judge and I have entered numerous orders in this FLSA collective action; there is no need to rehash the factual background. Defendant's motion is denied, for the reasons stated here.

The first discovery category at issue pertains to resumes, cover letters, and job applications Plaintiffs submitted to subsequent employers, as well as "notes taken by employers during [Plaintiffs'] job interviews" (doc. 204 at 8). The motion is denied as moot as to this topic. Plaintiffs have already produced their resumes to Defendant, and Defendant deposed Plaintiffs about them (doc. 220 at 4). Additionally, the only case Defendant cites from this judicial district in support of its request is one that grants in part a motion to compel a non-party employer to produce personnel records in response to a subpoena. *See Benavides v. Velocity IQ, Inc.*, No. 8:05–cv–1536–T–30, 2006 WL 680656, at *2–3 (M.D.Fla. Mar. 15, 2006). Defendant has not subpoenaed the information from Plaintiffs' subsequent employers and instead seeks it from Plaintiffs themselves. But according to Plaintiffs, they have no other information to produce, a fact they apparently testified to at deposition. Consequently, without ruling on whether the requested information is discoverable, I find that the issue is moot.

Next, through interrogatories and document production requests, Defendant seeks all posts to Plaintiffs' social media accounts from 2010 to the present that relate to "any job descriptions or similar statements about this case or job duties and responsibilities or hours worked which Plaintiffs posted on LinkedIn, Facebook or other social media sites." (Doc. 204 at 11). This request includes all private messages Plaintiffs sent from these sites (*Id.* at 12). Defendant

claims the information is relevant to its affirmative defense that Plaintiffs are not entitled to overtime compensation due to their exempt status, and "because [posts] are party admissions regarding plaintiff's job duties, responsibilities, and/or hours worked at Defendant—precisely the issues to be litigated in this case." (Doc. 204 at 11). Plaintiffs also may have posted comments which contradict their testimony in the case about breaks and hours worked, according to Defendant.

I agree with Plaintiffs that this request is too broad. Generally, social media content is neither privileged nor protected by any right of privacy. *Davenport v. State Farm Mut. Auto. Ins. Co.*, No.3:11–cv–632–J–JBT, 2012 WL 555759, at *1 (M.D.Fla. Feb. 21, 2012); *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387, 388 (E.D.Mich.2012). Nonetheless, Defendant "does not have a generalized right to rummage at will through information that Plaintiff has limited from public view." *Davenport*, 2012 WL 555759, at *2 (quoting *Tompkins*, 278 F.R.D. at 388). Although discovery provisions are broadly and liberally construed, a request still must be tailored to appear "reasonably calculated to lead to the discovery of admissible evidence." Rule 26(b)(1). Defendant has not met this threshold showing.

Defendant relies on *Higgins v. Koch Development Corporation*, No. 3:11–cv–81–RLY–WGH, 2013 WL 3366278, at *2 (S.D.Ind. July 5, 2013), a case in which plaintiffs sued a theme park for physical injuries they sustained on a ride. During discovery, the theme park asked for the plaintiffs' social media postings. *Id.* The plaintiffs refused, and the district court

[18 F.Supp.3d 1348]

granted the park's motion to compel. *Id.* at *3. The plaintiffs had alleged that their injuries severely impacted their abilities to enjoy life, engage in outdoor activities, and find jobs. Consequently, the plaintiffs' posts were discoverable. *Id.* at *2. The court in *Romano v. Steelcase, Inc.*, 30 Misc.3d 426, 907 N.Y.S.2d 650, 656 (N.Y.Super.2010), which Defendant also cites, reached a similar holding in a case in which the plaintiff's physical condition was in controversy.

But here, Plaintiffs' physical condition is not at issue. *Cf. Davenport*, 2012 WL 555759, at *2 (granting motion to compel as to tagged Facebook photos because the plaintiff's physical condition was at issue). Whether or not an opt-in Plaintiff made a Facebook post during work hours or about work has no bearing on total hours worked or whether their job position qualifies for an exemption under the FLSA. Additionally, the burden of requiring all of the opt-in Plaintiffs to review all of their postings on potentially multiple social media sites over a period of four years and determine which posts relate to their job, hours worked, or this case, would be "an extremely onerous and time-consuming task." *Jewell v. Aaron's, Inc.*, No. 1:12–cv–0563, 2013 WL 3770837, at *3 (N.D.Ga. July 19, 2013) (finding, in FLSA case, defendant-employer not entitled to discovery of social media posts, because it had not shown relevance of the information, and to produce it would be too burdensome). This is especially so when Defendant has nothing more than its "hope that there might be something of relevance" in the social media posts. *Id.* (citation and quotation omitted). Although some of the Plaintiffs testified to reading social media at some point during their work day, this does not, in and of itself, transform

Plaintiffs' social media posts into discoverable information. Additionally, some of the information Defendant seeks is protected from public view (for example, private Facebook messages). Defendant's speculation that the social media messages might include a party admission, without more, is not a sufficient reason to require Plaintiffs to provide Defendant open access to their communication with third parties. *Salvato v. Miley,* No. 5:12–cv–635–Oc–10PRL, 2013 WL 2712206, at *2 (M.D.Fla. June 11, 2013). This is my finding despite that Defendant has narrowed the scope of its request to seek only social media information relating to this case and Plaintiffs' job.[1]

The final issue is Defendant's request for records of Plaintiffs' banking, credit and debit card transactions, telephone activity, and travel. Defendant argues the records are relevant because they will show the dates and times Plaintiffs were engaged in non-work activities. Defendant has agreed to limit its request to "portions of the records showing the dates and times of transactions and enough information showing that the transactions were not work-related." (Doc. 204 at 12).

This discovery is too broad and hinges on the hope of finding something—anything—relevant to this litigation. Defendant relies on a case that is not on all fours with this one. In *Mancuso v. Florida Metropolitan University*, No. 09–61984–CIV, 2011 WL 310726, at *3–4 (S.D.Fla. Jan. 28, 2011), a FLSA case, the court granted in part and denied in part a plaintiff's motion to quash subpoenas that the employer-defendant had issued to plaintiff's bank. The court ordered the bank to produce plaintiff's un-redacted records to

[18 F.Supp.3d 1349]

plaintiff, and plaintiff to redact the records to show only the dates and times of transactions before producing them to defendant. *Id.* The parties in *Mancuso* agreed from the outset that the banking records were relevant (and the court did not address this); the plaintiff's only objection was to certain definitions included in the subpoenas. *Id.* at *1.

Defendant, again, has not met its threshold burden under Rule 26(b)(1). Plaintiffs admitted at deposition that they used debit and credit cards during vacation and non-work times. From this, Defendant deduces that any time Plaintiffs used their debit or credit cards, they were not working. This leap of logic is insufficient support for Defendant's broad request. Defendant is hoping to discover financial records that reveal Plaintiffs conducted personal banking during work hours.[2] Even if they did, this is not the smoking gun Defendant seems to think it is; Plaintiffs may have engaged in personal banking during breaks from work. And although neither party focuses on Defendant's request for Plaintiffs' cell phone records, the motion is denied on this topic as well. The parties do not dispute that Defendant was the cellular provider for Plaintiffs and provided them phones to use for work purposes (doc. 220 at 5). Thus, Defendant already has access to the telephone records it seeks from Plaintiffs.

Conclusion

For the reasons stated here, Defendant's motion to compel (doc. 204) is DENIED.

Notes:

[1.] Defendant also asks Plaintiffs to identify the social media sites they used during their employment with Defendant because it may be "necessary to subpoena these social media providers for such information." (Doc. 204 at 12). Discovery has closed. Any subpoenas would be untimely.

[2.] For example, Defendant contends that the financial records " *may* show that Plaintiffs took a lunch break, had discretion to attend to non-work activities during the day, or took vacations or other time off from work during the tines they now are claiming to have worked." (Doc. 204 at 14) (emphasis added). This is too speculative to support the broad nature of the discovery Defendant seeks.

907 N.Y.S.2d 650
30 Misc.3d 426

Kathleen ROMANO, Plaintiff,
v.
STEELCASE INC. and Educational & Institutional Cooperative Services Inc., Defendants.

Supreme Court, Suffolk County, New York.

Sept. 21, 2010.

JEFFREY ARLEN SPINNER, J.

[30 Misc.3d 427]

ORDERED, that Defendant STEELCASE's motion is hereby granted as set forth herein below.

Defendant STEELCASE moves this Court for an Order granting said Defendant access to Plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information upon the grounds that Plaintiff has placed certain information on these social networking sites which are believed to be inconsistent with her claims in this action concerning the extent and nature of her injuries, especially her claims for loss of enjoyment of life.

The present application was brought on by Order to Show Cause. The Court has

[907 N.Y.S.2d 652]

reviewed the submissions both in favor of and in opposition to the relief sought, as well as the applicable federal statutory law, specifically the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, which prohibits an entity, such as Facebook and MySpace from disclosing such information without the consent of the owner of the account (*see,* 18 U.S.C. § 2702(b)(3); *Flagg v. City of Detroit,* 252 F.R.D. 346 [E.D. Mich.2008]).

SCOPE OF PERMISSIBLE DISCOVERY

Pursuant to CPLR 3101, there shall be full disclosure of all non-privileged matter which is material and necessary to the defense or prosecution of an action. To this end, trial courts have broad discretion in the supervision of discovery, and in determining what is "material and necessary" (*see: Allen v. Crowell-Collier Pub. Co.,* 21 N.Y.2d 403, 288 N.Y.S.2d 449, 235 N.E.2d 430 [1968]; *Andon v. 302-304 Mott Street Assocs.,* 94 N.Y.2d 740, 709 N.Y.S.2d 873, 731 N.E.2d 589 [2000]; *Cabellero v. City of New York,* 48 A.D.3d 727, 853 N.Y.S.2d 165 (2 Dept. 2008). Within the context of discovery, "necessary" has been interpreted as meaning "needful and not indispensable" (*see: Allen* at 407, 288 N.Y.S.2d 449, 453, 235 N.E.2d 430). The "material and necessary" standard is to be interpreted liberally requiring disclosure of "any facts bearing on the controversy which will assist preparation for trial by sharpening the issues and reducing delay and prolixity. The test is one of usefulness and reason" (*see: Allen, supra; Andon, supra; Hoenig v. Westphal,* 52 N.Y.2d 605, 439 N.Y.S.2d 831, 422 N.E.2d 491 [1981] (pre-trial discovery is to be encouraged, limited only by the test of materiality of "usefulness and reason")).

[30 Misc.3d 428]

Each discovery request is to be decided on a case-by-case basis keeping in mind the strong public policy in favor of open disclosure (*see: Andon* at 747, 709 N.Y.S.2d 873, 878, 731 N.E.2d 589). If the information sought is sufficiently related to the issues in litigation so as to make the effort to obtain it in preparation for trial reasonable, then discovery should be permitted (*see: Allen* at 406-407, 288 N.Y.S.2d 449, 452, 235 N.E.2d 430; *In re Beryl,* 118 A.D.2d 705, 499 N.Y.S.2d 980 [2 Dept. 1986]). It is immaterial that the information sought may not be admissible at trial as "pretrial discovery extends not only to proof that is admissible but also to matters that may lead to the disclosure of admissible proof" (*see: Twenty Four Hour Fuel Oil Corp. v. Hunter Ambulance Inc.,* 226 A.D.2d 175, 640 N.Y.S.2d 114 [1 Dept. 1996]; *Polygram Holding Inc. v. Cafaro,* 42 A.D.3d 339, 839 N.Y.S.2d 493 [1 Dept. 2007] (disclosure extends not only to admissible proof but also to testimony or documents which may lead to the disclosure of admissible proof including materials which may be used in cross-examination")).

INFORMATION SOUGHT FROM INTERNET SITES

Plaintiffs who place their physical condition in controversy, may not shield from disclosure material which is necessary to the defense of the action (*see: Hoenig v. Westphal, supra*). Accordingly, in an action seeking damages for personal injuries, discovery is generally permitted with respect to materials that may be relevant both to the issue of damages and the extent of a plaintiff's injury (*see: Walker v. City of New York,* 205 A.D.2d 755, 614 N.Y.S.2d 31 [2 Dept.

1994]). including a plaintiff's claim for loss of enjoyment of life (*see: Orlando v. Richmond Precast Inc.*, 53 A.D.3d 534, 861 N.Y.S.2d 765 [2 Dept. 2008]) (in an action to recover damages for personal injuries, records sought were material and necessary to the defense

[907 N.Y.S.2d 653]

regarding plaintiff's claim of loss of enjoyment of life); *Vanalst v. City of New York*, 276 A.D.2d 789, 715 N.Y.S.2d 422 [2 Dept. 2000]; *Mora v. St. Vincent's Catholic Med. Ctr.*, 8 Misc.3d 868, 800 N.Y.S.2d 298 [Sup. Ct. NY. Co. 2005].

Thus, in *Sgambelluri v. Recinos*, 192 Misc.2d 777, 747 N.Y.S.2d 330 [Sup. Ct. Nassau Co. 2002], an action arising out of a motor vehicle accident, the court held that plaintiff's wedding video taken two years after the incident was clearly relevant to the claim of permanency of injuries. As a result of the accident, plaintiff alleged that she sustained permanent injuries to her neck and back, and testified at her deposition that she can no longer participate in certain activities such as running or horseback riding. Defendant sought a copy of her wedding video on the basis that it might have shown plaintiff in various activities such as dancing, which would be relevant to the claims. Plaintiff objected on

[30 Misc.3d 429]

the basis of the personal nature of the video. The court decided in favor of disclosure noting its relevancy to the claim of permanency of injuries. In so finding, the court reasoned that although the video is not a surveillance tape, as contemplated by CPLR § 3101(i), its:

> [L]anguage is broad enough to encompass any film, photograph or videotape ... involving a person referred to in paragraph one of subdivision (a), i.e., a party. This is consistent with the general policy of New York courts allowing liberal disclosure. Moreover, the 1993 addition of subdivision (i) only strengthens the argument for open disclosure. *Id.* at 779, 747 N.Y.S.2d 330, 332 (*internal quotations omitted*).

Like the plaintiff in *Sgambelluri*, Plaintiff herein also claims she sustained permanent injuries as a result of the incident and that she can no longer participate in certain activities or that these injuries have effected her enjoyment of life. However, contrary to Plaintiff's claims, Steelcase contends that a review of the public portions of Plaintiff's MySpace and Facebook pages reveals that she has an active lifestyle and has traveled to Florida and Pennsylvania during the time period she claims that her injuries prohibited such activity. In light of this, Defendant sought to question Plaintiff at her deposition regarding her MySpace and Facebook accounts, to no avail and following those depositions, served Plaintiff with a Notice for Discovery & Inspection requesting, *inter alia*, "authorizations to obtain full access to and copies of Plaintiff's current and historical records/information on her Facebook and MySpace accounts." Plaintiff has refused to provide the requested authorizations.

Both Facebook and MySpace are social networking sites where people can share information about their personal lives, including posting photographs and sharing information

about what they are doing or thinking. Indeed, Facebook policy states that "it helps you share information with your friends and people around you," and that "Facebook is about sharing information with others." [1] Likewise, MySpace is a "social networking service that allows Members to create unique personal profiles online in order to find and communicate with old and news friends;" and, is self-described as an "online community" where "you can share photos, journals and interests with your growing network

[30 Misc.3d 430]

of mutual friends," [2] and, as a "global lifestyle

[907 N.Y.S.2d 654]

portal that reaches millions of people around the world." [3] Both sites allow the user to set privacy levels to control with whom they share their information.

The information sought by Defendant regarding Plaintiff's Facebook and MySpace accounts is both material and necessary to the defense of this action and/or could lead to admissible evidence. In this regard, it appears that Plaintiff's public profile page on Facebook shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed. In light of the fact that the public portions of Plaintiff's social networking sites contain material that is contrary to her claims and deposition testimony, there is a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action. Preventing Defendant from accessing to Plaintiff's private postings on Facebook and MySpace would be in direct contravention to the liberal disclosure policy in New York State.

Although there is no New York case law directly addressing the issues raised by this application, there are instructive cases from other jurisdictions. Recently, in *Ledbetter v. Wal-Mart Stores Inc.*, (06-cv-01958-WYD-MJW, 2009 WL 1067018 [D. Colo. April 21, 2009]), defendant store sought, via subpoena, production of the content of plaintiffs' social networking sites.[4] Information contained on the public access areas contradicted plaintiffs allegations regarding the effect of their injuries on their daily lives. When the networking sites refused to provide the information absent plaintiffs' consent or request, defendant moved to compel production and plaintiffs moved for a protective order. Both plaintiffs had claimed physical and psychological injuries as a result of the accident which gave rise to lawsuit. By Order dated April 21, 2009, Magistrate Judge Watnabe denied plaintiffs' motion and held that the information sought by the subpoenas

[30 Misc.3d 431]

was "reasonably calculated to lead to the discovery of admissible evidence and is relevant to the issues in the case."

Likewise, in *Leduc v. Roman*, 2009 CarswellOnt 843 (February 20, 2009), a matter

pending in the Superior Court of Justice, Ontario, Canada, defendant also requested production of the plaintiff's Facebook pages, including, private pages. Plaintiff claimed that as a result of injuries allegedly sustained in a car accident, his enjoyment for life had lessened. Canadian law requires that each party disclose every document relating to any matter in the action over which he has possession or control absent a claim of privilege. Plaintiff had failed to disclose the information which defendant only learned about following a defense psychiatric examination. After only being able to access the limited portions of plaintiff's public profile page, defendant sought an order requiring production of all site materials as well as preservation of the materials. The decision denying the request was reversed on appeal, with the appellate court disagreeing that defendant was on a fishing expedition. In this regard, Judge Brown noted that it was "beyond controversy" that a person's Facebook pages may contain relevant documents (at ¶ 23); that other Canadian

[907 N.Y.S.2d 655]

cases had permitted into evidence photographs posted on a person's Facebook page showing them engaged in activities despite their claim to the contrary; and, it is reasonable to infer from the social networking purpose of Facebook, that even if a person only maintains a private profile with the public profile merely listing their name, that relevant information exists on their limited-access private pages (at ¶ 36). In deciding to permit the examination into the private Facebook profile, the court set forth:

> To permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.

(see also: Kent v. Laverdiere, 2009 CanLII 16741 (ON S.C., April 14, 2009) (as plaintiff asserted that accident disfigured her and lessened her enjoyment of life, any photos on Facebook or MySpace showing her in healthy state, enjoying life, would be relevant); *Bishop v. Minichiello,* 2009 BCSC 358 (CanLII, April 7, 2009) (defendant's motion for production of

[30 Misc.3d 432]

plaintiff's computer's hardrive so it could analyze how much time plaintiff spent on Facebook granted as the information sought was relevant to the issues in the case); *Goodridge v. King*, 2007 CanLII 51161 (ON S.C. October 30, 2007) (in action in which plaintiff claimed various injuries including loss of enjoyment of life and disfigurement following a car accident, photos posted by plaintiff on her Facebook account was evidence to the contrary, showing her socializing and dating); *Kourtesis v. Horis,* 2007 CanLII 39367 (ON S.C. September 24, 2007) (in proceeding concerning costs, court noted that during trial, Facebook photos of plaintiff were important element of case; apparently plaintiff testified that she no longer had a social life because of her injuries, yet the photographs taken after the accident, showed her at a party) [5].

Thus, it is reasonable to infer from the limited postings on Plaintiff's public Facebook and MySpace profile pages, that her private pages may contain materials and information that are relevant to her claims or that may lead to the disclosure of admissible evidence. To deny Defendant an opportunity access to these sites not only would go against the liberal discovery policies of New York favoring pre-trial disclosure, but would condone Plaintiff's attempt to hide relevant information behind self-regulated privacy settings.

PLAINTIFF'S PRIVACY CONCERNS

Production of Plaintiff's entries on her Facebook and MySpace accounts would not be violative of her right to privacy [6], and any such concerns are outweighed by Defendant's need for the information.

The Fourth Amendment's right to privacy, protects people, not places (*see: Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 [1967]) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.") In determining whether a right to privacy exists via the Fourth Amendment, courts apply the reasonableness

[30 Misc.3d 433]

standard set forth in the concurring opinion of Justice

[907 N.Y.S.2d 656]

Harlan in *Katz*: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable." *Id.* at 361, 88 S.Ct. 507, 516 (Harlan, J. concurring) (internal quotations omitted).

New York courts have yet to address whether there exists a right to privacy regarding what one posts on their on-line social networking pages such as Facebook and MySpace. However, whether one has a reasonable expectation of privacy in internet postings or e-mails that have reached their recipients has been addressed by the Second Circuit, which has held that individuals may not enjoy such an expectation of privacy (*see: U.S. v. Lifshitz,* 369 F.3d 173 [2 Cir.2004] citing *Guest v. Leis,* 255 F.3d 325 [6 Cir.2001]):

> Users would logically lack a legitimate expectation of privacy in materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer whose expectation of privacy ordinarily terminates upon delivery of the letter."

Likewise, whether one has a reasonable expectation of privacy in e-mails and other writings that have been shared with others, including entries on Facebook and MySpace, has been addressed by the United States District Court of New Jersey, which ordered such entries produced in *Beye v. Horizon Blue Cross Blue Shield of New Jersey,* 06-5337 (D.N.J. December

14, 2007). In this regard, the court stated that "[t]he privacy concerns are far less where the beneficiary herself chose to disclose the information." As to the entries which had not been shared with others, they were to be preserved. At issue in *Beye,* were on-line journals and diary entries of minor children who had been denied health care benefits for their eating disorders (*see also: Moreno v. Hanford Sentinel Inc.*, 172 Cal.App.4th 1125, 91 Cal.Rptr.3d 858 (Ct.App. 5 Dist.2009) (no person would have reasonable expectation of privacy where person took affirmative act of posting own writing on MySpace, making it available to anyone with a computer and opening it up to public eye); *Dexter v. Dexter,* 2007 WL 1532084, 2007 Ohio App LEXIS 2388 (Ohio Ct. App. Portage Co. 2007) (no reasonable expectation of privacy regarding MySpace writings open to public view).

[30 Misc.3d 434]

Indeed, as neither Facebook nor MySpace guarantee complete privacy, Plaintiff has no legitimate reasonable expectation of privacy. In this regard, MySpace warns users not to forget that their profiles and MySpace forums are public spaces [7], and Facebook's privacy policy set forth, *inter alia,* that:

> You post User Content ... on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable.

Further that:

> When you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos ... may be shared with others in accordance with the privacy settings you select. All such sharing of information is done at your own risk. Please keep in mind that if you disclose personal information in you profile or when posting comments,

[907 N.Y.S.2d 657]

> messages, photos, videos, Marketplace listing or other items, this information may become publicly available.[8]

Thus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, "[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking." [9]

Further, Defendant's need for access to the information outweighs any privacy concerns

that may be voiced by Plaintiff. Defendant has attempted to obtain the sought after information

[30 Misc.3d 435]

via other means e.g., via deposition and notice for discovery, however, these have proven to be inadequate since counsel has thwarted Defendant's attempt to question Plaintiff in this regard or to obtain authorizations from Plaintiff for the release of this information. The materials including photographs contained on these sites may be relevant to the issue of damages and may disprove Plaintiff's claims. Without access to these sites, Defendant will be at a distinct disadvantage in defending this action.

ORDERED, that Defendant STEELCASE's motion for an Order granting said Defendant access to Plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information, is hereby granted in all respects; and it is further

ORDERED, that, within 30 days from the date of service of a copy of this Order, as directed herein below, Plaintiff shall deliver to Counsel for Defendant STEELCASE a properly executed consent and authorization as may be required by the operators of Facebook and MySpace, permitting said Defendant to gain access to Plaintiff's Facebook and MySpace records, including any records previously deleted or archived by said operators; and it is further.

ORDERED, that Counsel for the moving party herein is hereby directed to serve a copy of this order, with Notice of Entry, upon Counsel for all the remaining parties and Non-Party FACEBOOK, within twenty (20) days of the date this order is entered by the Suffolk County Clerk.

[1] Facebook Principles- http: www. facebook. com/ policy. php (last visited April 3, 2009).

[2] About Us-MySpace.com/index.dfm?fuseaction=misc.aboutus (last visited June 16, 2009).

[3] MySpace Safety Highligh ts- http:// www. myspace. com/ index. cfm? frseaction= cms. veiwpage & placement=safety (last visited June 18, 2009).

[4] Facebook, MySpace and Meetup.com

[5] See, Charles Foster, *Uncovering the Truth:Social Networks are a Treasure Trove of Information,* Claims Canada, October/November 2008, http: www. claimscanada. ca. (last viewed June 18, 2009).

[6] In New York, there is no common law right to privacy. *See, Cordero v. NYP Holdings, Inc.*, 20 Misc.3d 1108(A), 866 N.Y.S.2d 90, 2008 WL 2522631 (Sup.Ct. N.Y. Co.2008).

[7] MySpace General Tips-ht tp:// www. myspace. com/ index. cfm? frseaction= cms. veiwpage & placement=safety-pagetips (last visited June 18, 2009).

[8] Facebook Principles-effective as November 26, 2008-http:// www. facebook. com/ policy.

php. last viewed June 18, 2009.

[9] Dana L. Flemming and Josheph M. Herlihy, *Department: Heads Up: What Happens When the College Rumor Mill Goes OnLine? Privacy, Defamation and Online Social Networking Sites*, 53 B.B.J. 16 (January/February, 2009).

2012 NY Slip Op 22175

The People of the State of New York
v.
Malcolm Harris, Defendant

2011NY080152

Criminal Court of the City of New York, New York County

Decided on June 30, 2012

Matthew A. Sciarrino Jr., J.

Twitter, Inc. ("Twitter") seeks to quash the January 26, 2012 subpoena issued by the New York County District Attorney's Office and upheld by this court's April 20, 2012 order. That order required Twitter to provide any and all user information, including email addresses, as well as any and all tweets posted for the period of September 15, 2011 to December 31, 2011, from the Twitter account @destructuremal, which was allegedly used by Malcolm Harris. This is a case of first impression, distinctive because it is a criminal case rather than a civil case, and the movant is the corporate entity (Twitter) and not an individual (Harris). It also deals with tweets that were publicly posted rather than an e-mail or text that would be directed to a single person or a select few.

On October 1, 2011, the Defendant, Malcolm Harris, was charged with Disorderly Conduct (Penal Law §240.20 [5]) after allegedly marching on the roadway of the Brooklyn Bridge. On January 26, 2012, the People sent a *subpoena duces tecum* to Twitter seeking the defendant's account information and tweets for their relevance in the ongoing criminal investigation (CPL 610; Stored Communications Act [18 USC §2703(c)(2)]). On January 30, 2012, Twitter, after conferring with the District Attorney's office, informed the defendant that the Twitter account @destructuremal had been subpoenaed. On January 31, 2012, the defendant notified Twitter of his intention to file a motion to quash the subpoena. Twitter then took the position that it would not comply with the subpoena until the court ruled on the defendant's motion to quash the subpoena and intervened.

On April 20, 2012, this court held that the defendant had no proprietary interest in the user information on his Twitter account, as he lacked standing to quash the subpoena (*See* CPLR 1012 [a], 1013; *People v Harris*,__NYS2d__, 2012 NY Slip Op 22109 [Crim Ct, NY County 2012]). This court ordered Twitter to provide certain information to the court for *in camera*

review to safeguard the privacy rights of Mr. Harris.

On May 31, 2012 David Rosenblatt, a member of Twitter's Board of Directors, was personally served within New York County with a copy of this Court's April 20, 2012 order, a copy of the January 26, 2012 trial subpoena, and a copy of the March 8, 2012 trial subpoena. Twitter subsequently moved to quash the April 20, 2012 court order. To date, Twitter has not complied with this court's order.

***Discussion*:**

Twitter is a public, real-time social and information network that enables people to share, communicate, and receive news. Users can create a Twitter profile that contains a profile image**,** background image, and status updates called tweets, which can be up to 140-characters in length on

the website.[1] Twitter provides its services to the public at large. Anyone can sign up to use Twitter's services as long as they agree to Twitter's terms. Twitter is a Delaware corporation with its principal place of business in California.

The Stored Communications Act ("SCA") (18 USC §2701 *et seq.*) defines and makes distinctions between Electronic Communication Service ("ECS") versus Remote Computing Service ("RCS"), and content information versus non-content information. ECS is defined as "any service that provides the user thereof the ability to send or receive wire or electronic communication." (*See* 18 USC §2510[15]). RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."(*see* 18 USC § 2711[2]). The Wire Tap Act (18 USC §2510[8]) defines content information as "contents, when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." In contrast, logs of account usage, mailer header information (minus the subject line), list of outgoing e-mail addresses sent from an account, and basic subscriber information are all considered to be non-content information.[2]

While Twitter is primarily an ECS (as discussed in *Harris,*__NYS2d__ ,at 6), it also acts as a RCS. It collects and stores both non-content information such as IP addresses, physical locations, browser type, subscriber information, etc. and content information such as tweets. The SCA grants greater privacy protections to content information because actual contents of messages naturally implicate greater privacy concerns than network generated information about those communications.[3]

1.Twitter Users and Standing to Challenge Third-Party Disclosure Request

Twitter argues that users have standing to quash the subpoena. The issue is whether Twitter users have standing to challenge third-party disclosure requests under the terms of service that existed during the dates in question. In *Harris,* (*id*. at 7) the New York City Criminal Court held that a criminal defendant did not have standing to quash a subpoena issued to a third-party

online social networking service because the defendant has no proprietary interest. The court's decision was partially based on Twitter's then terms of service agreement. After the April 20, 2012 decision, Twitter changed its terms and policy effective May 17, 2012. The newly added portion states that: "You Retain Your Right To Any Content You Submit, Post Or Display On Or Through The Service." (*See* Twitter, *Terms of Service*, https://twitter.com/tos/ [accessed June 11, 2012]).

Twitter argues that the court's decision to deny the defendant standing places an undue burden on Twitter. It forces Twitter to choose between either providing user communications and account information in response to all subpoenas or attempting to vindicate its users' rights by moving to quash these subpoenas itself.However, that burden is placed on *every* third-party respondent to a subpoena (*see In Re Verizon*, 257 F Supp 2d 244, 257-258 [2003]; *United States v Kennedy*, 81 F Supp 2d 1103, 1110 [2000]) and cannot be used to create standing for a defendant where none exists.

The Stored Communications Act (18 USC §2703 [d]) states:

> A court issuing an order pursuant to this section, on a motion made promptly by ***the service provider, may quash or modify such order***, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider. (*Emphasis added).*

In the defense motion they also reference a concurrence by J. Sotomayor who said that "it may be necessary for the court to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" (*see United States v Jones*, 565 US __, 132 S Ct 957 [2012]).Publication to third parties is the issue. Tweets are not e-mails sent to a single party. At best, the defense may argue that this is more akin to an e-mail that is sent to a party and carbon copied to hundreds of others. There can be no reasonable expectation of privacy in a tweet sent around the world.[4] The court order is not unreasonably burdensome to Twitter, as it does not take much to search and provide the data to the court.[5] So long as the third party is in possession of the materials, the court may issue an order for the materials from the third party when the materials are relevant and evidentiary (18 USC §2703[d]; *People v Carassavas*, 103 Misc 2d 562 [Saratoga County Ct 1980]).

Consider the following: a man walks to his window, opens the window, and screams down to a young lady, "I'm sorry I hit you, please come back upstairs." At trial, the People call a person who was walking across the street at the time this occurred. The prosecutor asks, "What did the defendant yell?" Clearly the answer is relevant and the witness could be compelled to testify. Well today, the street is an online, information superhighway, and the witnesses can be the third party providers like Twitter, Facebook, Instragram, Pinterest, or the next hot social media application.

2. The Court Order, Federal Law and New York State Law

The second issue is whether the court order was a violation of the Fourth Amendment, the

Federal Stored Communications Act, or any other New York law.

The Fourth Amendment

To establish a violation of the Fourth Amendment, the defendant must show either (1) a physical intrusion onto defendant's personal property; or (2) a violation of a defendant's reasonable expectation of privacy. (*see United States v Jones* (132 S Ct 945, 950 [2012]; *Kyllo v United States*, 533 US 27, 33 [2001] .) In *Jones (id.* at 949), the U.S. Supreme Court held that the government's installation of a Global Positioning System ("GPS") tracking device on a target's vehicle to obtain information was a physical intrusion on a constitutionally protected area. In *People v Weaver* (12 NY3d 433 [2009])theNew York Court of Appeals heldthat the placing of a GPS tracking device inside the bumper of the defendant's vehicle, by a state police investigator, was a physical intrusion. However, in this case there was no *physical* intrusion into the defendant's Twitter account. The defendant had purposely broadcast to the entire world into a server 3,000 miles away. Therefore, the defendant's account is protected by the Fourth Amendment *only* if "the government violated a subjective expectation of privacy that society recognizes as reasonable." (*see Kyllo v United States*, 533 US 27, 33 [2001], citing *Katz v United States*, 389 US 347, 361 [1967]).[6]

The Supreme Court has repeatedly held that the Fourth Amendment does not protect information revealed by third parties. (*see United States v Miller*, 425 US 435, 443 [1976].) Several courts have applied this rationale and held that internet users do not retain a reasonable expectation of privacy. In *Romano v Steelcase Inc.*, (30 Misc 3d 426 [Sup Ct, NY County 2010])the court held that "users would logically lack a legitimate expectation of privacy in materials intended for publication or public posting."[7]

If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world. This is not the same as a private email, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the internet that now exist.

Those private dialogues would require a warrant based on probable cause in order to access the relevant information.

Interestingly, in 2010, Twitter signed an agreement with the Library of Congress providing that every public tweet from Twitter's inception and beyond would be archived by the Library of Congress.[8] Also, Twitter's Privacy Policy states in part:

> Our Services are primarily designed to help you share information with the world. Most of the information you provide us is information you are asking us to make public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet, and many other bits of information that result from your use of the Services. (see Twitter, Twitter Privacy

Policy https://twitter.com/privacy [accessed June 11, 2012].)

There is no reasonable expectation of privacy for tweets that the user has made public. It is the act of tweeting or disseminating communications to the public that controls. Even when a user deletes his or her tweets there are search engines available such as "Untweetable", "Tweleted" and "Politwoops" that hold users accountable for everything they had publicly tweeted and later deleted.[9]

Therefore, the defendant's Fourth Amendment rights were not violated because there was no physical intrusion of the defendant's tweets and the defendant has no reasonable expectation of privacy in the information he intentionally broadcast to the world.

Stored Communications Act The SCA's requirements for a court order states that:

A court order for disclosure under subsection (b) or (c)....shall be issued only if the government entity offers specific and articulate facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or ***the records or other information sought, are relevant and materials to an ongoing criminal investigation.*** (*Emphasis added*) (*see* 18 USC §2703[d]).

The defendant's anticipated trial defense is that the police either led or escorted him onto the non-pedestrian part of the Brooklyn Bridge, a defense allegedly contradicted by his publicly posted tweets around the time of the incident. In *Harris*, (*id.* at 7-8) the court held that the information sought was relevant. The April 20, 2012 court order was issued to comply with the January 26, 2012 subpoena.

The People are seeking two types of information, non-content information such as subscriber information, e-mail addresses, etc. and content information such as tweets. The SCA protects only private communications[10] and allows disclosure of electronic communication when it's not overbroad.[11]

In general, court orders have no limitations on the types of information to be disclosed (18 USC §2703[d]). The SCA mandates different standards that the government must satisfy to compel a provider to disclose various types of information (18 USC §2703). To compel a provider of ECS to disclose contents of communication in its possession that are in temporary "electronic storage" for 180 days or less, the government must obtain a search warrant (18 USC §2703[a]). A court order must compel a provider of ECS to disclose contents in electronic storage for greater than 180 days or to compel a provider of RCS to disclose its contents (18 USC §2703[a], [b], and [d]). The law governing compelled disclosure also covers the above mentioned non-content records. The rules are the same for providers of ECS and RCS and the government can obtain a §2703(d) order to compel such non-content information (18 USC §2703 [c][1][B]).

The non-content records such as subscriber information, logs maintained by the network server, etc. and the September 15, 2011 to December 30, 2011 tweets are covered by the court

order. However, the government must obtain a search warrant for the December 31, 2011 tweets.

New York State Law

The scope of a *subpoena duces tecum* is sufficiently circumscribed when: (1) the materials are relevant and evidentiary; (2) the request is specific; (3) the materials are not otherwise procurable reasonably in advance of trial by the exercise of due diligence; (4) the party cannot properly prepare for trial without such a production and inspection in advance of trial and the failure to obtain such inspection may tend unreasonably to delay the trial; and (5) the application is made in good faith and is not intended as a general "fishing expedition" *(People v Carassavas*, 103 Misc 2d 562 [Saratoga County Ct 1980], citing *People v Price*, 100 Misc 2d 372, 379 [1979]). The District Attorney seeks the subpoenaed information to refute Harris's anticipated trial defense. In *Harris*, (*id.* at 7-8) the court agreed that the *subpoena duce tecum* was sufficiently circumscribed and a court order was issued on April 20, 2012 to comply with the subpoena.

On May 31, 2012 David Rosenblatt, a member of Twitter's Board of Directors, was personally served within New York County with a copy of this court's April 20, 2012 order, a copy of the January 26, 2012 trial subpoena, and a copy of the March 8, 2012 trial subpoena. There are no jurisdictional issues and there are no violations of the New York Constitution.

***Conclusion*:**

In dealing with social media issues, judges are asked to make decisions based on statutes that can never keep up with technology.[12] In some cases, those same judges have no understanding of the technology themselves (Stephanie Rabiner, Esq., Technologist, *Do Judges Really Understand Social Media?* http://blogs.findlaw.com/technologist/2012/05/do-judges-really-understand-social-media.html [May 9, 2012]). Judges must then do what they have always done - balance the arguments on the scales of justice. They must weigh the interests of society against the inalienable rights of the individual who gave away some rights when entering into the social contract that created our government and the laws that we have agreed to follow. Therefore, while the law regarding social media is clearly still developing, it can neither be said that this court does not understand or appreciate the place that social media has in our society nor that it does not appreciate the importance of this ruling and future rulings of courts that may agree or disagree with this decision. In recent years, social media has become one of the most prominent methods of exercising free speech, particularly in countries that do not have very many freedoms at all.

The world of social media is evolving, as is the law around it. Society struggle with policies, whether they are between student and teacher (NYC Department of Education, *NYC Department of Education Social Media Guidelines)*,[13] or the right of a company to examine an applicant's Facebook page as part of the interview process (Bill Chappell, *State Approves Bill to Ban Employers From Seeking Facebook Login Info*, http://www.npr.org/blogs/thetwo-way/2012/04/10/150354579/state-approves-bill-to-ban-employers-from-seeking-facebook-login-info). As the laws, rules and societal norms evolve and change with each new advance in

technology, so too will the decisions of our courts. While the U.S. Constitution clearly did not take into consideration any tweets by our founding fathers, it is probably safe to assume that Samuel Adams, Benjamin Franklin, Alexander Hamilton and Thomas Jefferson would have loved to tweet their opinions as much as they loved to write for the newspapers of their day (sometimes under anonymous pseudonyms similar to today's twitter user names). Those men, and countless soldiers in service to this nation, have risked their lives for our right to tweet or to post an article on Facebook; but that is not the same as arguing that those public tweets are protected. The Constitution gives you the right to post, but as numerous people have learned, there are still consequences for your public posts. What you give to the public belongs to the public. What you keep to yourself belongs only to you.

Accordingly, the motion to quash is granted in part and denied in part. The court finds in favor of the People for all non-content information and content information in ECS and RCS from September 15, 2011 to December 30, 2011. However, ECS content information less than 180 days old (tweeted on December 31, 2011) may only be disclosed pursuant to a search warrant, and the court decision in *People v Harris* is so modified. That search warrant should be requested of a judge of competent jurisdiction. However, to avoid any issue of alleged non-impartiality, that warrant should be made to another judge of this court.

Accordingly, it is hereby:

ORDERED, that Twitter disclose all non-content information and content information from September 15, 2011 to December 30, 2011; and it is further

ORDERED, that the materials be provided to this court for *in camera* inspection. The relevant portions thereof will be provided to the office of the District Attorney, who will provide copies to the defense counsel as part of discovery; and it is further

ORDERED, that the clerk of this court notify the Presiding Judge of Jury 2 of the receipt of the materials.

This opinion shall constitute the decision and order of the Court.

Notes:

[1.] (*See Guidelines for Law Enforcement*, https://support.twitter.com/entries/41949-guidelines-for-law-enforcement/ [accessed May 30, 2012].)

[2.] Orin Kerr, Comment, *A User's Guide to the Sored Communications Act, and the Legislator's Guide to Amending It*, 72 Geo Wash L Rev 1208 [2004].

[3.] *Id*. at 9.

[4.] In fact, on August 1, 2012 your tweets will be sent across the universe to a galaxy far, far

away. (*see* Chris Taylor, Mashable Social Media, *Your Tweets to Be Beamed Across Space. Will ET RT?*, http://mashable.com/2012/06/26/et-rt/ [June 26, 2012]).

[5.] The general New York rule is that only the recipient of a subpoena in a criminal case has standing to quash it. (*see People v Lomma*, 2012 WL 309327 at *5-6 [Sup Ct, NY County 2012], citing *People v Doe*, 96 AD2d 1018, 1019 [1st Dept 1983] [banking and telephone records]; *People v Crispino*, 298 AD2d 220, 221 [1st Dept 2002] ["defendant, as a customer, has no proprietary interest" in the defendant's bank account records]).

[6.] See also, People v. Suleman, (NYLJ July 13, 2011 at *1 [Crim Ct, NY County] [Decided on 6/22/2011]) where the court held that the taxicab owner had no reasonable expectation of the information generated and stored by a GPS device in the cab.

[7.]Twitter argues that the court should embrace the holding in *United States v Warshak*, (631 F3d 266 [6th Cir 2010]). In *Warshak*, the court found that the defendant had a reasonable expectation of privacy in his e-mails. However, the *Warshak* case is distinguishable from the case at hand because the former deals with private e-mails as opposed to public postings. *Warshak* did not address public communications at all; instead the court held only that "e-mail requires strong protections under the Fourth Amendment."(*Warshak*, 631 F3d at 286). If such Fourth Amendment protections were to extend to *public* postings, it would undermine the very basis of the *Warshak* holding.

[8.] (*See* Matt Raymond, Library of Congress, *How Tweet It Is!: Library Acquires Entire Twitter Archive*, http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/ [accessed May 30, 2012]). The Twitter community received the initial heads up via their own feed @librarycongress. Twitter has its users' consent for disclosure to the Library of Congress by virtue of its Private Policy. The Library of Congress' archives is not yet available due to its high volume of composition of billions of tweets, and with an estimate of 140 million new tweets per day. (*see* Audrey Watters, *How the Library of Congress is Building the Twitter Archive*, http://radar.oreilly.com/2011/06/library-of-congress-twitter-archive.html [accessed June 11, 2012].*)*

[9.] *See http://untweetable.com;http://tweleted.com/ and http://mashable.com/2012/05/30/poliwoops/.*

[10.] *(See Kaufman v Nest Seekers, LLC, 2006 WL 2807177 at *5 [SDNY 2006] [Only electronic bulletin boards which are not readily accessible to the public are protected under the SCA]; Knop v Hawaiian Airlines Inc., 302 F3d 868, 875 [9th Cir 2002]["The legislative history of the Electronic Communications Protection Act suggest that Congress wanted to protect electronic communication that are configured to be private, such as e-mail and private electronic communications."]; Snow v DirecTV, Inc., 450 F3d 1314, 1320-21 [11th Cir 2006] [holding that the SCA does not apply to materials that is readily available to the public.]*

[11.] *Orin Kerr, Comment, A User's Guide to the Sored Communications Act, and the Legislator's Guide to Amending It, 72 Geo Wash L Rev 1208 [2004].*

[12.] *The SCA was enacted in 1986 and mainly applied to the start of e-mails. The SCA was*

enacted long before the creation of Twitter and the concept of blogging which started in 2006.

[13.] *http://schools.nyc.gov/NR/rdonlyres/BCF47CED604B-4FDDB752DC2D81504478/0/DOESocialMediaGuidelines20120430.pdf*

RESOURCES

K&L Gates Electronic Discovery Law Database: https://ediscovery.klgates.com/search.aspx

Kroll Discovery Searchable Database: http://www.ediscovery.com/pulse/case-law/

Twitter Advanced Search: https://twitter.com/search-advanced

Social Mention: http://www.socialmention.com/

Buzzumo: https://app.buzzsumo.com/research/most-shared

Social Searcher: https://www.social-searcher.com/

DISCOVERY, AUTHENTICATION AND ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

SPEAKERS:
BROOKE BARNETT-BERNAL, MICHAEL A. PATTERSON
AND EDWARD J. WALTERS JR.

SATURDAY, JULY 23, 2016 • 8 - 9 AM

BATON ROUGE BENCH BAR

CONFERENCE 2016

DISCOVERY, AUTHENTICATION AND ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

PRESENTED BY

Michael A. Patterson
S. Brooke Barnett-Bernal
Long Law Firm, LLP
4041 Essen Lane, Suite 500
Baton Rouge, Louisiana 70809

Edward J. Walters, Jr.
Walters, Papillion, Thomas, Cullens, LLC
12345 Perkins Rd
Baton Rouge, Louisiana 70810
JULY 2016

TABLE OF CONTENTS

MICHAEL A. PATTERSON is a graduate of the LSU Law Center and is the senior litigation partner with Long Law Firm in Baton Rouge, Louisiana. He received a Certificate and LLM in Dispute Resolution from Pepperdine University. He is the managing member of The Patterson Resolution Group which provides mediation and arbitration services throughout the State of Louisiana in complex legal matters. He serves on the adjunct faculty of the LSU Law Center and, along with Ed Walters, teaches a course in trial advocacy and evidence. He is the author of many legal articles and is the chapter author of *Louisiana Trial Procedure, Hearsay*. He is a past president of the Louisiana State Bar Association and the Baton Rouge Bar Association. He is past Chairman of the Louisiana Supreme Court Committee on Bar Admissions. He received the LSU Law Center Distinguished Achievement Award in 2013.

BROOKE BARNETT-BERNAL is a partner with the Long Law Firm, L.L.P. in Baton Rouge, Louisiana. Mrs. Bernal attended Louisiana State University, where she graduated summa cum laude with a Bachelor of Arts degree in 2003 and a Bachelor of Science degree in 2004. Mrs. Bernal double majored in Spanish and International Trade and Finance. In May 2007, she graduated from Louisiana State University's Paul M. Hebert Law Center, earning a Juris Doctorate degree and a Bachelor of Civil Law degree. During law school, she clerked for Long Law Firm and since joining the firm, her clients have included accountants, attorneys, architects, engineers, small business owners and government agencies. Mrs. Bernal is an active member of the LSBA and BRBA and currently serves on the LSBA Legislation Committee and BRBA Bench Bar Committee, among others. She is the co-author of the Ins and Outs of Rule 19 – How it Works and What You Need to Know (LSU Law Center CLE, October 2009), Construction Legislation 2010 Indemnity Clauses in Construction Contracts (BRBA Construction Law CLE Seminar, March 2011), and ESI: Electronically Stored Information – Securing, Safeguarding, Submitting and Screwups (Spoliation) (LSBA Uncorked: A CLE Adventure in California's Wine Country, March 2014). Mrs. Bernal was named as a "Rising Star" by Louisiana Super Lawyers in 2015 and 2016.

EDWARD J WALTERS, JR. a partner in the Baton Rouge law firm of Walters, Papillion, Thomas, Cullens, received his B.S. from LSU in 1969 and his J.D. from the LSU Law Center in 1975. He has practiced in the Baton Rouge area for over 38 years representing plaintiffs in personal injury cases. He is Board Certified in Civil Trial Advocacy and Civil Pretrial Advocacy by the National Board of Trial Advocates and is a Fellow of the American College of Trial Lawyers and the International Academy of Trial Lawyers. He is an Adjunct professor of law at the LSU Law Center where he and Mike Patterson jointly teach a trial skills course entitled "Advanced Trial and Evidence Seminar." He is a frequent lecturer and writer on litigation, evidence, ethics and professionalism topics and has been the editor of the Baton Rouge Bar Association's monthly magazine *Around the Bar* for over 28 years.

I. INTRODUCTION

A lack of understanding, fear and outright prejudice against social media has resulted in a hodgepodge of mostly ad hoc decisions which illustrate a failure of the bench and bar to grasp how these sites work. This lack of understanding has resulted in overly restrictive discovery limitations, overly broad discovery of this type of information, and the exclusion of evidence that clearly meets the requirements of La. Code Evid. art. 901. A better understanding will assist all members of the bench and bar.

II. THE DISCOVERY OF SOCIAL MEDIA

Social media content is playing an ever increasing role in litigation due to its near ubiquitous presence. There are over 2 billion Facebook users. Adults between 25 and 34 comprise 30% of users. The high usage of social media has not gone unnoticed by the practicing trial and bench bar. For instance, a recent survey of members of the American Academy of Matrimonial Attorneys found 66% had indicated they have found evidence on Facebook.[1]

The early cases involving discovery of social media sites has been decidedly mixed. For example, in a Pennsylvania state court case, *Mazzarella v. Mount Airy #1, LLC,*[2] a premises liability case, the plaintiff objected to a discovery request seeking the username and password on the grounds of privacy. The court, ruling on a motion to compel, simply said the information requested could lead to relevant information. The court further stated those that use social media waive an expectation of privacy.

In an employment discrimination case, a federal magistrate judge ordered the production of social media account passwords, reasoning that social media was like a file folder called

[1] John G. Browning, *Digging for Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU SCI. & TECH. L. REV 465, 467 (2011).
[2] 2012 WL 6000678 (Pa.Com.Pl. 11/7/12).

"Everything About Me," which individuals voluntarily shared with others. Therefore, the presumption is that it should be produced.[3]

In another case, *Beswick v. North West Medical Center, Inc.,* the defendant submitted an interrogatory asking for the plaintiff's social media username and password. The court found such a request was sufficiently specific. The court further stated the plaintiff's entire private Facebook account was discoverable because it was clearly relevant.[4]

Another equally unsatisfactory approach taken by courts, where a party is seeking access to a litigant's social media, requires a preliminary showing by the mover that the public portion of a litigant's social media site has relevant information (which contradicts the position taken in the suit). If such a showing is made, then complete access to the remainder of the litigant's site is granted. A good example of this approach is *Romano v. Steelcase.*[5] In that case, the plaintiff claimed her injuries largely confined her to her house and bed. There were photos on the public portion of her page contradicting that allegation. As a result, the court ordered the plaintiff to execute a consent to Facebook and MySpace granting defendants access to all of plaintiff's social media information.

However, in *Tompkins v. Detroit Metropolitan Airport,*[6] a plaintiff claimed physical injuries from a slip and fall at the Detroit airport. The defendant sought access to the private portion of the plaintiff's Facebook page, claiming the public content postings conflicted with the claims in the lawsuit. To support the request, the defendants relied on a photo of the plaintiff at a birthday party holding a very small dog. However, the court rejected the request, finding the photo was not inconsistent with the claims. The court denied any access to the private Facebook content.

---

[3] *EEOC v. Original Honeybaked Ham Co. of Georgia*, Inc., 2012 WL 5430974, at *1 (D. Colo. Nov. 7, 2012).
[4] 2011 WL 7005038 (Fla. 17th Cir. Ct. Nov. 3, 2011).
[5] 907 N.Y.S. 2d 650 (Sup. Ct. Suffolk County 2010).
[6] 278 F.R.D. 387, 388-89 (E.D. Mich. 2012).

A. *IN CAMERA* REVIEW

Another approach is to order the parties to provide the court with the user's password directly.[7] In *Barnes v. CUS Nashville, LLC,* the court ordered a non-party witness to accept the magistrate judge as a Friend on Facebook so that an *in camera* review of the Facebook contents could take place.[8]

B. STORED COMMUNICATION ACT[9]

Parties may not obtain the content of a user's social media page directly from the social media company without the user's consent. However, the act does not protect users from being ordered by a court to give consent.[10]

C. PRIVACY

Privacy settings are an integral feature of social media sites. Public means that anyone who goes to the website can see the information. Private limits the audience to selected viewers. The public or private nature of the content is meaningless when discussing discovery. A private setting does not make that material off limits to discovery. Although users expect some privacy for "private" content areas, courts have held there is no constitutional right, common law protection or statutory privilege that protects "private" social media content from discovery.[11] There are two legal principles at play in the issue of privacy. The first principle is the reasonable expectation test and the second is the third-party disclosure rule. These legal principles make it difficult to argue that information is private when it is posted to a social media account which exists for the purpose of sharing information with other people.

---

[7] *Offenback v. L.M. Bowman, Inc.*, 2011 WL 2491371, at *1-2 (M.D. Pa. June 22, 2011).
[8] *Barnes v. CUS Nashville, LLC*, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).
[9] 18 U.S.C. Sec. 2701 (2012).
[10] Orin S. Kerr, *A User's Guide to the Stored Communication Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213 (2004).
[11] *Trail v. Lesko*, 2012 WL 2864004 (Pa. Ct. Com. Pl. July 5, 2012).

In *United States v. Jones,* Justice Sotomayor, in concurrence, made these observations:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to a third party. This approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers, the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post,* at 962, and perhaps not. One doubts that people would accept without complaint the warrantless disclosure to the government of a list of every website they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. One would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

132 S.Ct. 945, 957 (2012) (concurring opinion).

D. THE ANSWER: PROPORTIONALITY

Social media should be handled like any other form of evidence. The producing party bears the burden of determining what is responsive and needs to be produced. The discovery request should be drafted in a way that includes all forms of social media and is sufficiently narrowly drawn. All discovery requests that seek social media evidence should be specified to closely relate to the litigation.

In re Air Crash Near Clarence Ctr., N.Y. on Feb. 12, 2009 is a good example of how a requesting party should draft the request.[12] In that case, the defendant requested the production of all electronic communications during a certain time period, "including social media accounts, emails, text messages and instant messages," that were related to the plaintiff's domicile on the date of the crash.

[12] 2011 WL 6370189, at *6 (W.D.N.Y. Dec. 20, 2011).

The most recent amendment to Fed. R. Civ. P. 26 probably will solve some of the issues in the current case law. Rule 26(b)(1) defines the scope of discovery as "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." The rule identifies six factors to be considered in determining whether the discovery is proportional to the needs of the case. They include the importance of the issues at stake, the amount in controversy, the relative access to information, the parties' resources, the importance of the discovery and whether the burden or expense outweighs its likely benefit. Privacy settings could be considered in weighing the "burden" of proposed discovery that could outweigh the marginal benefit of that information.

E. SOME THOUGHTS ON SNAPCHAT

Snapchat is an application intended to facilitate self-destructing video, photo, or chat communications.[13] When a user sends a photo he or she sets a timer that sets how many seconds the viewer can see the photo before it disappears from the screen. The maximum time is ten seconds. Normally, the viewer will only be able to view the Snapchat once before it disappears.

A party is under an affirmative obligation to preserve all relevant social media once he or she is placed on notice that another party is seeking information in the private sections of the party's social media accounts. It seems that in the Snapchat discovery arena, the biggest questions will be how to prove relevance and spoliation.

Currently, there is no consistent method to retrieve a sender's Snapchat history.[14] A litigant using Snapchat during litigation, or where litigation is foreseen, can simply push the save button

[13] Larry Magid, *What is Snapchat and Why Do Kids Love It and Parents Fear It?* (updated), FORBES.COM (May 1, 2013, 4:14 PM), http://perma.cc/8WPA-57KG.
[14] Molly McHugh, *Yes You Can Recover Dead Snapchats and Here's the Video Proof*, DIGITAL TRENDS (May 19, 2013), http://perma.cc/JLK8-PZYE.

to preserve the Snap. If she fails to do so, a court will likely find some fault with a resulting sanction.

III. AUTHENTICATION AND ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

The admissibility of social media evidence remains a prevalent issue in litigation today. To be admissible, social media evidence, like any other kind of evidence, must (1) be relevant, (2) be authentic, (3) be non-hearsay, (4) meet the original writing requirement and (5) not be unfairly prejudicial. Determining whether social media evidence is relevant or whether its probative value outweighs its prejudicial effect does not require a different analysis than for more traditional types of evidence. Pamela E. Carter & Shelley K. Napolitano, *Social Media: An Effective Evidentiary Tool*, 61 La. B. J. 332, 334 (2014). However, social media evidence does require "new considerations in the areas of authentication, hearsay and form." *Id.*

A. AUTHENTICATION.

Information obtained from the internet was once viewed by many courts as inherently unreliable and untrustworthy. For example, in *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, the United States District Court for the Southern District of Texas famously referred to the "evidence" the plaintiff sought to introduce from the Internet as "voodoo information." 76 F. Supp. 2d 773, 774-775 (S.D. Tex. 1999). In fact, the court reacted to the plaintiff's attempt to rely on such information with extreme skepticism, stating:

> While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo and misinformation. . . . Anyone can put anything on the Internet. No website is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation . . . .

Id. While the concerns echoed by the United States District Court for the Southern District of Texas in *St. Clair* still exist, many courts have relaxed their views about the reliability and trustworthiness of the information obtained from the internet and social media websites.

No laws have been enacted to specifically and separately address the authentication of social media evidence. Instead, most courts have adapted the traditional rules of evidence to determine whether information obtained from social media websites, such as Facebook and Twitter, is authentic. Carter & Napolitano, *Social Media*, 61 La. B. J. at 334; *See also*, *Smith v. State,* 136 So. 3d 424, 432 (Miss. 2014).

The authentication standard for both Louisiana and federal courts requires that the evidence be "sufficient to support a finding that the matter in question is what its proponent claims." La. C.E. art. 901(a); Fed. R. Evid. Art. 901(a). Authentication is a condition precedent to admissibility. *Id*. Louisiana Code of Evidence Article 901(b), like its federal counterpart, provides a non-exclusive list of methods for authenticating evidence.

Preliminary questions about whether evidence is authentic, and thus, admissible, are determined by the judge. La. C.E. art. 104(a); Fed. R. Evid. 104(a); *State v. Robertson,* 2012-0743 (La. App. 1 Cir. 12/21/12); 2012 WL 6681830, at *8. When the proponent of the evidence makes a *prima facie* showing of authenticity, the evidence goes to the jury, which will ultimately determine how much weight, if any, should be given to the evidence. Honorable Paul W. Grimm, Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. 433, 458 (2013). On the other hand, if the judge is presented with plausible evidence of both authenticity and inauthenticity, he is faced with a conditional relevance issue under Rule 104(b). *Id.* at 460; *See also*, *Lorraine v. Markel Am. Ins. Co.,* 241 F.R.D. 534, 539-

540 (D.Md. 2007).[15] In that case, the judge should admit the evidence and allow the jury to ultimately resolve whether the evidence admitted is that which the proponent claims. *Id; See also*, Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 460-461; *State v. Smith,* No. 2015-K-1359 (La. App. 4 Cir. 4/20/16).

When dealing with social media evidence, courts have struggled with consistently applying a uniform standard, and essentially, two approaches have emerged. One approach sets a high bar for authentication by only allowing the evidence to be admitted if the court definitively determines the evidence is authentic. The other approach sets a lower bar for the admissibility of social media evidence and focuses on whether there is sufficient evidence for a reasonable juror to conclude the evidence is authentic. Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 441, 449.

The more stringent approach for the authentication of social media evidence is best exemplified in *Griffin v. State,* 419 Md. 343, 19 A.3d 415 (Md. 2011). In *Griffin*, the State used printouts from the public MySpace profile of the defendant's girlfriend, which contained the statement "FREE BOOZY [defendant's nickname]!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!," to show she had threatened the State's key witness prior to trial by posting that warning on her MySpace page. *Id.* at 362-363. The State did not question the girlfriend about the post in question; rather, the State only offered the testimony of its lead investigator in an attempt to authenticate her MySpace profile page. *Id.* at 348-351. The investigator testified he knew it was the girlfriend's MySpace page from the photograph of her and the defendant (Boozy) on the front, through references to Boozy and their children, and from her birth date shown on the page. *Id*.

[15] Authentication under Rule 901 is viewed as a subset of relevancy, because "evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not that which its proponent claims."

The Maryland Supreme Court observed that, with "relative ease," a person "can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password." *Id.* at 352-353. Therefore, the court concluded that, considering "[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user," a printout from a social media account "requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site." *Id.* at 357-358. Accordingly, the Maryland Supreme Court held the photograph of the defendant's girlfriend, coupled with her personal information and references to "freeing Boozy," were not sufficient "distinctive characteristics" on a MySpace profile page to authenticate its printout, given the possibility that someone other than the girlfriend not only could have created the MySpace account but also posted the "snitches get stiches" comment. *Id.*

The court then identified three proper methods of authenticating printouts of postings from social media sites. The first method is to ask the purported creator if he created the profile and also if he authored the posting in question, i.e., "testimony of a witness with knowledge that the offered evidence is what it is claimed to be." *Id.* at 363; *See also*, La. C.E. art. 901(b)(1); Fed. R. Evid. 901(b)(1). The second method is to search the computer of the alleged owner of the social media account, and examine the computer's internet history and hard drive to determine whether that computer was used to generate the profile page and posts in question. The third option is to obtain information directly from the social media network provider to connect the profile to the person who allegedly created it and the posts in question to the person who allegedly authored them. *Id.* at 363-364.[16]

[16] In *Sublet v. State*, the Maryland Supreme Court appears to have adopted a less stringent standard than the one announced in *Griffin.* 442 Md. 632, 113 A.3d 695 (Md. 2015). First, the court specifically noted the three methods

Similarly, in *Commonwealth v. Williams*, a witness testified the defendant's brother –using the MySpace screen name "doit4it" – contacted her through four instant messages on her MySpace page to tell her not to testify against the defendant or to claim a lack of memory regarding the events at her apartment the night of the murder (with which the defendant was charged). 926 N.E.2d 1162, 1165, 1172 (Mass. 2010). The trial court admitted the witness' testimony about the messages but did not admit the printouts of the brother's MySpace page. The Supreme Judicial Court of Massachusetts analogized the MySpace messages to a phone call, stating that "a witness's testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, is insufficient evidence to admit the call as a conversation with 'A.'" *Id.* at 1172. In addition, the court noted the State did not offer any evidence about "how secure such a Web page is, who can access a MySpace page, whether codes are needed for such access, etc." *Id.* at 1172-1173.

The court concluded that while the State laid sufficient foundation to establish the messages were sent by someone with access to the MySpace account of the defendant's brother, "it did not identify the person who actually sent the communication." *Id.* Nor did the State produce any expert testimony to show that no one other than the defendant's brother could communicate from his MySpace page. *Id.* Therefore, the court held the trial court should not have admitted the witness' testimony regarding the MySpace messages because there was insufficient evidence presented by the State to authenticate them. *Id.* at 1173.

---

for authenticating social media postings articulated in *Griffin* were *non-exclusive*. Second, the court expressly stated it was embracing the standard for authenticating social media evidence adopted by the United States Court of Appeals for the Second Circuit in *United States v. Vayner,* 769 F.3d 125 (2nd Cir. 2014), i.e., that the authentication "requirement is satisfied if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification." *Id.* at 664, 666-667. Under this standard, preliminary determinations about authentication are made by the trial judge as to whether "the proof advanced is sufficient to support a finding that the item in question is what its proponent claims it to be…so that a reasonable juror could find in favor of authenticity." *Id.* at 666.

Likewise, in *State v. Eleck*, the defendant tried to impeach one of the State's witnesses, Simone Judway, with private messages purporting to be sent from her Facebook account. 130 Conn.App. 632, 635, 23 A.3d 818, 820 (Conn.App. Ct. 2011). The defendant, using his own testimony to authenticate printouts of the Facebook messages, stated that (1) he downloaded and printed the messages directly from his own computer, (2) the username "Simone Danielle" belonged to the witness, (3) the Facebook profile contained photographs and other entries identifying the witness as the creator of the account, and (4) when he logged into his Facebook account after the previous day's testimony, he had been removed from her list of friends. *Id.* at 635-636, 820-821. The State's witness testified that, although the messages came from her Facebook account, her account had been "hacked" and she had been unable to access it for some time. *Id.* at 635, 820. The trial court refused to admit the Facebook messages and the Appellate Court of Connecticut affirmed, explaining:

> The need for authentication arises in this context because an electronic communication, such as a Facebook message, an e-mail or a cell phone text message, could be generated by someone other than the named sender. This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended. Additionally, passwords and website security are subject to compromise by hackers. Consequently, proving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship.

Id. at 638-639, 822-823. Even though the appellate court noted the witness' testimony - that her Facebook account had been "hacked" - was "dubious under the particular facts at hand, given that the messages were sent before the alleged hacking of the account took place," it found her testimony highlighted the general lack of security of social media sites and raised the issue as to whether a third party could have sent the messages from her Facebook account. *Id.* at 642, 824.

These decisions appear to harbor the same skepticism regarding information obtained from the Internet and social media sites as did the U.S. District Court for the Southern District of Texas in *St. Clair*.[17] In the second line of cases, courts more appropriately evaluate whether there is sufficient evidence of authenticity for a reasonable jury to conclude the social media evidence is what the proponent claims it to be. Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 449. The judge acts as the gatekeeper and the jury is the ultimate decision maker regarding the authenticity of social media evidence. *Id.* at 456-461; *See also*, *Campbell v. State,* 382 S.W. 3d 545, 549 (Tex.App. – Austin 2012).

For instance, in *Campbell,* over the defendant's objection, the trial court admitted a printout of private messages the defendant purportedly sent from his Facebook account to his girlfriend, whom he was accused of assaulting. *Campbell,* 382 S.W.3d at 548. To authenticate the messages, the State offered the testimony of the girlfriend, who stated she (1) had received the Facebook messages from the defendant a few days after the alleged assault, (2) did not send the messages to herself, and (3) did not have access to defendant's Facebook account after the alleged assault. *Id.* at 551. The appellate court noted that "printouts of emails, internet chat room dialogues, and text messages have all been admitted into evidence when found to be sufficiently linked to the purported author so as to justify the admission to the jury for its ultimate determination." *Id.* at 549. However, the appellate court observed that:

> [W]ith respect to identity, Facebook presents an authentication concern that is twofold. First, because anyone can establish a fictitious profile under any name, the person viewing the profile has no way of knowing whether the profile is legitimate. Second, because a person may gain access to another person's account by obtaining the user's name and password, the person viewing communications on or from an account profile cannot be certain that the author is in fact the profile owner. Thus, the fact that an electronic communication on its face purports to originate from a certain person's social networking account is generally insufficient

[17] *See also*, *People v. Beckley,* 185 Cal.App. 4th 509, 110 Cal. Rptr. 3d 362 (2010).

> standing alone to authenticate that person as the author of the communication. (internal citations omitted).

Id. at 550. As a result, the court explained the most appropriate method for authenticating social media evidence, as with any other kind of evidence, "will often depend on the nature of the evidence and the circumstances of the particular case." *Id.*

In affirming the trial court's decision, the appellate court found the undisputed testimony showed (1) the defendant had a Facebook account, (2) only he and his girlfriend had access to that account, and (3) his girlfriend received messages from his Facebook account. The court further found the Facebook messages contained "distinctive characteristics," including speech that was consistent with the defendant's - a native of Jamaica - and references to the alleged assault and potential charges, "which at the time the messages were sent, few people would have known about." *Id.* at 551-552. While the court did note the evidence did not conclusively establish the defendant sent the messages, it held the State was not required to "rule out all possibilities inconsistent with authenticity or prove beyond any doubt that the evidence is what it purports to be." *Id.* at 552.

Similarly, in *Parker v. State,* the State used Facebook posts allegedly authored by the defendant after a physical altercation between her and the State's witness regarding a mutual love interest, to demonstrate the defendant's role in the incident and discredit her theory of self-defense. 85 A.3d 682, 683 (Del. 2014). The exhibit containing the defendant's Facebook posts also included her name, a photograph of her and a time and date stamp for each entry. *Id.* at 684. The State offered the testimony of the witness, who had "shared" or "reposted" the Facebook posts purportedly sent by the defendant on her own Facebook page, to authenticate them. *Id.* The trial court admitted the Facebook posts, finding the entries contained sufficient distinctive characteristics to satisfy Rule 901's authentication requirements. *Id.* In rendering its decision, the

trial court specifically rejected the more stringent approach adopted by the Maryland courts in favor of the more lenient rule adopted in Texas. The trial court noted Delaware follows the "distinguishing characteristics" rationale, which has allowed courts to authenticate handwritten letters of prisoners using solely the nicknames of the parties involved and references to the crimes, as well as emails using only the sender's email address. Therefore, the trial court determined the State had adequately authenticated the defendant's Facebook posts using witness testimony and circumstantial evidence. *Id.* at 688.

The Delaware Supreme Court affirmed the trial court's ruling and concluded social media evidence should be subject to the same authentication requirements under Rule 901 as any other evidence. *Id.* at 687. Therefore, the supreme court held that when a party seeks to introduce evidence obtained from social media networks, "he or she may use any form of verification under Rule 901 – including witness testimony, corroborative circumstances, distinctive characteristics or descriptions and explanations of the technical process or system that generated the information – to authenticate a social media post."[18] *Id.* at 687-688.

In a recent Mississippi Supreme Court case, the court cited to cases adopting the more stringent approach for authenticating social media evidence, as well as cases applying the more lenient standard, in holding the State had failed to adequately authenticate Facebook messages allegedly sent by the defendant. *Smith,* 136 So. 3d at 434-435. In *Smith,* the State presented evidence the Facebook account belonged to someone with the defendant's name, evidence the Facebook page contained a "grainy" photograph allegedly of the defendant, and testimony from a witness who said the defendant had sent the messages to her. *Id.* at 434. No other identifying information was provided and no testimony regarding the security of or access to the defendant's

[18] *See also*, *Tienda v. State,* 358 S.W.3d 633 (Tex.Crim.App. 2012); *State v. Assi,* 2012 WL 3580488 (Ariz. Ct. App. 8/21/12); *People v. Valdez,* 201 Cal.App.4th 1429, 135 Cal.Rptr.3d 628 (2011).

Facebook account was elicited (the court specifically noted the susceptibility of social media accounts to security breaches). *Id.* at 434-435.

The Mississippi Supreme Court concluded that "something more" other than a low-quality photograph and a name was needed to properly authenticate the Facebook account and messages in question. In its opinion, the Mississippi Supreme Court observed the court in *Tienda v. State* had surveyed cases involving the authentication of social media evidence and provided an illustration of what that "something more" may be to adequately present a prima face case of authentication, including:

> the purported sender admits authorship, the purported sender is seen composing the communication, business records of an internet service provider or cell phone company show that the communication originated from the purported sender's personal computer or cell phone under circumstances in which it is reasonable to believe that only the purported sender would have access to the computer or cell phone, the communication contains information that only the purported sender could be expected to know, the purported sender responds to an exchange in such a way as to indicate circumstantially that he was in fact the author of the communication, or other circumstances peculiar to the particular case. . .

Id. at 433, citing *Tienda v. State,* 358 S.W.3d 633, 639-641 (Tex.Crim.App. 2012). It is unclear which, if any, of the two approaches for authenticating social media evidence was adopted by the Mississippi Supreme Court in *Smith;* however, it appears the court applied a higher burden for the authentication of social media evidence than what is required by the more lenient approach embraced in Texas and Delaware, or any other states.

In Louisiana, all five appellate courts have allowed social media evidence to be admitted into evidence. Grant Guillot, *Evidentiary Implications of Social Media: An Examination of the Admissibility of Facebook, MySpace and Twitter Postings in Louisiana Courts,* 61 La. B.J. 338 (2014). For instance, in *Boudwin v. General Ins. Co. of America,* the plaintiffs were allegedly injured in an automobile accident but the jury did not award them any damages for past and future

mental pain and suffering, physical disability or loss of enjoyment of life and future medical expenses. 2011-2270 (La. App. 1 Cir. 9/14/11); 2011 WL 4433578. At trial, the plaintiffs were questioned about their Facebook posts and photographs from their Facebook profiles, which showed they routinely engaged in physical activities after the accident, including jogging, engaging in the P90X exercise program and playing softball. *Id.* at *3. The Louisiana First Circuit Court of Appeal upheld the jury award, noting "the record clearly shows that neither [plaintiffs] have experienced any significant limitations or impairments as a result of the injuries they sustained in the . . . accident." *Id.*

In addition, in *State v. Wood,* the Louisiana Third Circuit Court of Appeal upheld the trial court's finding there was no conspiracy between the defendant and his alleged co-conspirator based on the review of information obtained from cellphone records, computers, emails and MySpace and Facebook accounts belonging to the defendant and his alleged co-conspirators. 08-1511 (La. App. 3 Cir. 6/3/09); 11 So. 3d 701, 709-710. Furthermore, in *State v. Wiley,* the State offered the testimony of the mother of one of the co-defendants who identified the defendant and her son from several photographs posted to her son's MySpace page. 10-811 (La. App. 5 Cir. 4/26/11); 68 So.3d 583, 588. The State also called the manager of safety, security and compliance for MySpace.com as a witness to testify regarding the MySpace user numbers, user names and locations of the defendant and co-defendants, and that they were all MySpace friends with each other. *Id.* The Louisiana Fifth Circuit Court of Appeal found no error in the trial court admitting evidence related to the defendant and co-defendant's MySpace accounts. *Id.* at 591.

Even though each of the Louisiana courts of appeal have been required to determine the admissibility of social media evidence, there has been virtually no discussion by the courts as to

the requirements for the authentication of social media evidence, until very recently. *State v. Smith,* No. 2015-K-1359 (La. App. 4 Cir. 4/20/16).

In *Smith,* the Louisiana Fourth Circuit Court of Appeal was faced with the challenge of deciding the proper standard for the authentication of social media evidence under Louisiana law. *Id.* The State sought to introduce printouts containing a purported photograph of the defendant holding a gun and threatening messages allegedly made by the defendant to the victim. The State presented the testimony of only one witness – the investigating officer – who testified the victim had shown her the threatening "text messages" allegedly from the defendant on her cellphone; however, no testimony was offered to demonstrate how the messages had been copied or reproduced on paper. Furthermore, these so-called "text messages" were actually social media messages sent from an unknown social media platform, which the investigating officer could not identify. Moreover, the investigating officer testified she made no attempt to independently verify where the purported photograph of the defendant or social media messages had come from. *Id.*

In determining the appropriate standard to be applied in Louisiana, the Fourth Circuit specifically noted the authentication of social media evidence is an area of the law where "Louisiana courts have dispensed limited guidance." *Id.* As a result, the court of appeal looked to the approaches adopted by other state and federal courts for the authentication of social media evidence. Ultimately, the Fourth Circuit, relying on the Maryland Supreme Court's decision in *Sublet*, held the proper inquiry under Louisiana law "is whether the proponent has adduced

sufficient evidence to support a finding that the proffered evidence is what it is claimed to be." *Id.*;[19] *See also*, *Sublet,* 442 Md. at 678, 113 A.3d at 722.[20]

Applying this standard to the facts of *Smith,* the Louisiana Fourth Circuit Court of Appeal concluded the trial court had abused its discretion in ruling the social media evidence offered by the State was admissible. In reaching its decision, the court of appeal found the State had offered no evidence or testimony (1) to prove the defendant was the creator of the social media account, (2) as to whether the defendant, assuming he had, in fact, created the account, allowed others to access it using his password, or (3) of any "unique qualities" regarding the social media messages "from which one may assert [the defendant] sent the messages." *Id.* In fact, the Fourth Circuit found the State had "presented *no evidence at all* to authenticate the social media posts;" and instead, had simply asserted "it intend[ed] to authenticate the social media posts at trial." *Id.* Consequently, the court of appeal held the State failed to carry its burden of proof, and remanded the matter to the trial court to conduct an evidentiary hearing for the State to present evidence pursuant to La. C.E. art. 901 to authenticate the social media posts for the trial court to rule on their admissibility at trial. The Fourth Circuit expressly directed the trial court to determine, on remand, whether the State has supplied sufficient "evidence (direct or circumstantial) to support a reasonable jury conclusion that the evidence it seeks to introduce at trial is what the State purports it to be." *Id.*

[19] The Fourth Circuit noted that sufficient proof for authenticating social media evidence will vary from case to case, which proof may be direct or circumstantial; and thus, the type and quantum of evidence will depend on the context and the purpose of its introduction. The Fourth Circuit further noted that "evidence which is deemed sufficient to support a reasonable juror's finding that the proposed evidence is what it is purported to be in one case, may be insufficient in another."

[20] Whereby the Maryland Supreme Court concluded the appropriate standard in Maryland should be whether "there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be." This approach is different than the approach adopted four years earlier by the Maryland Supreme Court in *Griffin, supra.*

Because the bar for authentication of evidence is not particularly high, Louisiana courts should follow the more lenient approach for the authentication of social media evidence. This approach "affords the appropriate deference to the interplay between the evidence rules that govern the admissibility of social media evidence: Rule 104(a) and (b), Rule 901 and Rule 401." Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 456. Thankfully, the Louisiana Fourth Circuit Court of Appeal, in *Smith,* ***correctly*** decided to embrace the more lenient approach for the authentication of social media evidence, which has been adopted in Texas and Delaware, and more recently, in Maryland.

B. CHECKLIST FOR AUTHENTICATION

When it comes to authenticating social media evidence be prepared and plan ahead. There are three methods listed under La. C.E. art. 901(b) and Fed. R. Evid. 901(b) that are particularly applicable for authenticating social media evidence, including:

1. **Rule 901(b)(1) – Someone with Personal Knowledge**. If you are trying to authenticate someone's Facebook profile, call the person who created the account and ask if he or she made or authorized the postings in question.

2. **Rule 901(b)(3) – Use of an Expert or Comparison by Fact Finder**. This method would likely involve retaining a computer forensic expert to authenticate the social media account and subject postings. The downside to this method is it is costly, and further, it is difficult to predict how the jury would respond to the use of expert testimony to authenticate social media content.

3. **Rule 901 (b)(4) – Distinctive Circumstances or Characteristics.** This is may be one of the most useful ways to authenticate social media evidence. However, it requires a person who has personal knowledge of the social media content to explain how the social media evidence was created or an expert who can provide opinion testimony.

Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 468-472; *See also*, *Lorraine,* 241 F.R.D. at 545-548.[21]

[21] While many of the cases cited in *Lorraine* "involve digital evidence from Internet sites other than social media sites, the methods approved by those cases apply with equal force to social media evidence." Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence*, 36 Am. J. Trial Advoc. at 461.

In addition, in civil cases, if social media evidence was produced by the opposing party in response to a request for production, most courts will "recognize that there is presumption of authenticity." *Id.* at 468; *See also, Lorraine,* 241 F.R.D. at 552.[22] Furthermore, in civil cases, requests for admissions are a perfectly acceptable way to authenticate social media evidence. Finally, in all cases, parties can stipulate to the authenticity of social media evidence. *Id.*

C. HEARSAY.

There are no general hearsay guidelines when it comes to information obtained from social media websites. Carter & Napolitano, *Social Media*, 61 La. B. J. at 335. In order for the social media evidence to be considered hearsay, it must be a statement, made by a declarant, offered for the truth of the matter asserted, and not be excluded from the definition of hearsay or fall into one of the hearsay exceptions.[23] To qualify as a statement, there must be an assertion. *Id.* In *Perfect, 10 Inc. v. Cybernet Ventures, Inc.,* the court held images and text, which were introduced to show they were found on the defendant's website, were not "statements" because, in effect, they were not asserting anything. 213 F.Supp.2d 1146, 1155 (C.D. Cal. 2002). Similarly, in *Firehouse Rest. Grp, Inc. v. Scurmont, LLC*, the court concluded printouts of websites that merely depicted a logo or use of the word "firehouse" in a business name did not quality as "statements." 2011 WL 3555704, at *5 (D.S.C. Aug. 11, 2011).

Social media evidence is frequently offered to prove the truth of the matter asserted, i.e., to show the declarant was at a particular place at a particular time using photographs posted on Facebook or statements made on Twitter. But that is not always the case. For instance, in *U.S. v. Siddiqui,* the United States Court of Appeals for the Eleventh Circuit determined emails between

[22] Citing *Indianapolis Minority Contractors Ass'n v. Wiley*, 1998 WL 1988826, at *6 (S.D. Ind. May 13, 1998) ("The act of production is an implicit authentication of documents produced.")
[23] *Lorraine* provides a very thorough analysis of the various hearsay considerations involving ESI.

the defendant and a third-party had been admitted to show the relationship between the two that it was customary for them to communicate by email, not that the statements made in the emails were true; and thus, they were not hearsay. 235 F.3d 1318, 1323 (11th Cir. 2000).

If, on the other hand, social media evidence is being offered for the truth of the matter, it may fall into one of the hearsay exceptions or exclusions. Various hearsay exceptions and exclusions that may be applicable to social media evidence include: admissions of a party-opponent,[24] present sense impression,[25] excited utterance (will "OMG" be sufficient?),[26] then existing state of mind or condition.[27] Finally, watch out for multiple hearsay in social media evidence, such as "friends" of the declarant making statements on social media regarding statements made by the declarant or intentions of the declarant. Re-tweets on Twitter or re-posts on Facebook are simply repeating what someone else said and likely do not quality as admissions.

D. ORIGINAL WRITING REQUIREMENT

The original writing rule requires that an original or duplicate original be admitted into evidence "[t]o prove the content of a writing, recording, or photograph." La. C.E. arts. 1002 and 1003, Fed. R. Evid. Rules 1002 and 1003. A printout of a social media page can qualify as the "original" document or the "best evidence of computer-generated information." Carter & Napolitano, *Social Media*, 61 La. B. J. at 335. Indeed, both the Louisiana and federal rules of evidence provide that if "data [is] stored in or copied onto a computer or similar device . . . any printout or other output readable by sight, shown to reflect the data accurately, is an "original."'

[24] Carter & Napolitano, *Social Media*, 61 La. B. J. at 335; *See also*, *Siddiqui,* 235 F.3d at 1323*; Lorraine,* 241 F.R.D. at 567-568; *Perfect 10, Inc.,* 213 F.Supp.2d at 1155; *United States v. Safavian,* 435 F.Supp.2d 36 (D.D.C. 2006). Again, while most of these cases involve emails, the analysis should apply equally to social media evidence.
[25] La. C.E. art. 801(1); *See also, Lorraine,* 241 F.R.D. at 569-570. This exception "may be a gold mine for attorneys because many social media users have constant access to their accounts on their cell phones. Carter & Napolitano, Social Media, 61 La. B. J. at 335.
[26] La. C.E. art. 801(2); *See also, Lorraine,* 241 F.R.D. at 569-570.
[27] La. C.E. art. 801(3); *See also, Lorraine,* 241 F.R.D. at 570*; Safavian,* 435 F.Supp.2d at 44 (admitting e-mails that contained statements of defendant's state of mind under Rule 803(3)).

La. C.E. art. 1001; Fed. R. Evid. 1001. In fact, in *Laughner v. State,* the Indiana appellate court held a printout of an instant messaging conversation, which was copied and pasted into a blank document and then printed, met the original writing requirement. 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002), *abrogated (on other grounds)* by *Fajardo v. State,* 859 N.E.2d 1201 (Ind. 2007).

IV. CONCLUSION

Knowledge of how social media works is critical to the advocate. If you do not understand it, you cannot explain why it is discoverable or should be admissible to the court. You need to be prepared to "educate" the court a little more than you would expect in order to put the court at ease that the discovery is narrowly tailored to the specific issues in the case and the proffered exhibit is what it purports to be.