Evidence in Family Law Matters: Clearing Evidentiary Hurdles

Friday, September 16, 2016

Albany Marriott

CLE Course Materials and NotePad®

Complete course materials distributed in electronic format online in advance of the program.

Sponsored by the

New York State Bar Association and the Committee on Legal Aid

This program is offered for education purposes. The views and opinions of the faculty expressed during this program are those of the presenters and authors of the materials. Further, the statements made by the faculty during this program do not constitute legal advice.

Lawyer Assistance Program 800.255.0569

Q. What is LAP?

A. The Lawyer Assistance Program is a program of the New York State Bar Association established to help attorneys, judges, and law students in New York State (NYSBA members and non-members) who are affected by alcoholism, drug abuse, gambling, depression, other mental health issues, or debilitating stress.

Q. What services does LAP provide?

A. Services are **free** and include:

- Early identification of impairment
- Intervention and motivation to seek help
- Assessment, evaluation and development of an appropriate treatment plan
- Referral to community resources, self-help groups, inpatient treatment, outpatient counseling, and rehabilitation services
- Referral to a trained peer assistant – attorneys who have faced their own difficulties and volunteer to assist a struggling colleague by providing support, understanding, guidance, and good listening
- Information and consultation for those (family, firm, and judges) concerned about an attorney
- Training programs on recognizing, preventing, and dealing with addiction, stress, depression, and other mental health issues

Q. Are LAP services confidential?

A. Absolutely, this wouldn't work any other way. In fact your confidentiality is guaranteed and protected under Section 499 of the Judiciary Law. Confidentiality is the hallmark of the program and the reason it has remained viable for almost 20 years.

Judiciary Law Section 499 Lawyer Assistance Committees Chapter 327 of the Laws of 1993

Confidential information privileged. The confidential relations and communications between a member or authorized agent of a lawyer assistance committee sponsored by a state or local bar association and any person, firm or corporation communicating with such a committee, its members or authorized agents shall be deemed to be privileged on the same basis as those provided by law between attorney and client. Such privileges may be waived only by the person, firm or corporation who has furnished information to the committee.

Q. How do I access LAP services?

A. LAP services are accessed voluntarily by calling **800.255.0569** or connecting to our website **www.nysba.org/lap**

Q. What can I expect when I contact LAP?

A. You can expect to speak to a Lawyer Assistance professional who has extensive experience with the issues and with the lawyer population. You can expect the undivided attention you deserve to share what's on your mind and to explore options for addressing your concerns. You will receive referrals, suggestions, and support. The LAP professional will ask your permission to check in with you in the weeks following your initial call to the LAP office.

Q. Can I expect resolution of my problem?

A. The LAP instills hope through the peer assistant volunteers, many of whom have triumphed over their own significant personal problems. Also there is evidence that appropriate treatment and support is effective in most cases of mental health problems. For example, a combination of medication and therapy effectively treats depression in 85% of the cases.

Personal Inventory

Personal problems such as alcoholism, substance abuse, depression and stress affect one's ability to practice law. Take time to review the following questions and consider whether you or a colleague would benefit from the available Lawyer Assistance Program services. If you answer "yes" to any of these questions, you may need help.

1. **Are my associates, clients or family saying that my behavior has changed or that I don't seem myself?**
2. **Is it difficult for me to maintain a routine and stay on top of responsibilities?**
3. **Have I experienced memory problems or an inability to concentrate?**
4. **Am I having difficulty managing emotions such as anger and sadness?**
5. **Have I missed appointments or appearances or failed to return phone calls? Am I keeping up with correspondence?**
6. **Have my sleeping and eating habits changed?**
7. **Am I experiencing a pattern of relationship problems with significant people in my life (spouse/parent, children, partners/associates)?**
8. **Does my family have a history of alcoholism, substance abuse or depression?**
9. **Do I drink or take drugs to deal with my problems?**
10. **In the last few months, have I had more drinks or drugs than I intended, or felt that I should cut back or quit, but could not?**
11. **Is gambling making me careless of my financial responsibilities?**
12. **Do I feel so stressed, burned out and depressed that I have thoughts of suicide?**

There Is Hope

CONTACT LAP TODAY FOR FREE CONFIDENTIAL ASSISTANCE AND SUPPORT

The sooner the better!

Patricia Spataro, LAP Director

1.800.255.0569

New York State Bar Association

FORM FOR VERIFICATION OF PRESENCE AT THIS PROGRAM

Pursuant to the Rules pertaining to the Mandatory Continuing Legal Education Program for Attorneys in the State of New York, as an Accredited Provider of CLE programs, we are required to carefully monitor attendance at our programs to ensure that certificates of attendance are issued for the correct number of credit hours in relation to each attendee's actual presence during the program. Each person may only turn in his or her form-you may not turn in a form for someone else. Also, if you leave the program at some point prior to its conclusion, you should check out at the registration desk. Unless you do so, we may have to assume that you were absent for a longer period than you may have been, and you will not receive the proper number of credits.

Speakers, moderators, panelists and attendees are required to complete attendance verification forms in order to receive MCLE credit for programs. Faculty members and attendees: please complete, sign and return this form along with your evaluation, to the registration staff **before you leave** the program.

You MUST turn in this form at the end of the program for your MCLE credit.

Evidence in Family Law Matters: Clearing Evidentiary Hurdles
Friday, September 16, 2016 | New York State Bar Association's Committee on Legal Aid, Albany Marriott, Albany, NY

Name:
(Please print)

I certify that I was present for the entire presentation of this program

Signature: Date:

Speaking Credit: In order to obtain MCLE credit for speaking at today's program, please complete and return this form to the registration staff before you leave. **Speakers** and **Panelists** receive three (3) MCLE credits for each 50 minutes of presenting or participating on a panel. **Moderators** earn one (1) MCLE credit for each 50 minutes moderating a panel segment. Faculty members receive regular MCLE credit for attending other portions of the program.

NEW YORK STATE BAR ASSOCIATION

Live Program Evaluation (Attending In Person)

Please complete the following program evaluation. We rely on your assessment to strengthen teaching methods and improve the programs we provide. The New York State Bar Association is committed to providing high quality continuing legal education courses and your feedback is important to us.

Program Name: Evidence in Family LAw Matters: Clearing Evidentiary Hurdles

Program Code: FRIDVFA2

Program Location: Albany Marriott - Albany, NY

Program Date: September 16th 2016

1. What is your overall evaluation of this program? Please include any additional comments.
☐ Excellent ☐ Good ☐ Fair ☐ Poor

Additional Comments____

2. Please rate each Speaker's Presentation based on **CONTENT** and **ABILITY** and include any additional comments.

	CONTENT				ABILITY			
	Excellent	Good	Fair	Poor	Excellent	Good	Fair	Poor
Ellen C Schell	☐	☐	☐	☐	☐	☐	☐	☐
Ian Harris	☐	☐	☐	☐	☐	☐	☐	☐
Katherine Woodhouse McGerald	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐	☐	☐	☐

(please turn over)

Additional comments (CONTENT)

_____

_____

Additional comments (ABILITY)

_____

_____

3. Please rate the program materials and include any additional comments.
☐ Excellent ☐ Good ☐ Fair ☐ Poor

Additional comments

_____

_____

4. Do you think any portions of the program should be **EXPANDED** or **SHORTENED**? Please include any additional comments.
☐ Yes – Expanded ☐ Yes – Shortened ☐ No – Fine as is

Additional comments

_____

_____

5. Please rate the following aspects of the program: **REGISTRATION**; **ORGANIZATION**; **ADMINISTRATION**; **MEETING SITE** (if applicable), and include any additional comments.

	Please rate the following:				
	Excellent	Good	Fair	Poor	N/A
Registration	☐	☐	☐	☐	☐
Organization	☐	☐	☐	☐	☐
Administration	☐	☐	☐	☐	☐
Meeting Site (if applicable)	☐	☐	☐	☐	☐

Additional comments

_____

_____

6. How did you learn about this program?
☐ Ad in legal publication ☐ NYSBA web site ☐ Brochure or Postcard
☐ Social Media (Facebook / Google) ☐ Email ☐ Word of mouth

7. Please give us your suggestions for new programs or topics you would like to see offered

_____

_____

NEW YORK STATE BAR ASSOCIATION
One Elk Street, Albany, NY 12207
Phone: 518-463-3200 | Secure Fax: 518.463.5993

Evidence in Family Law Matters: Clearing Evidentiary hurdles – outline

2.5 MCLE credits in Skills; .5 MCLE credit in Ethics for both experienced and newly-admitted attorneys

2.5 Hours

1. Principles of Evidence and Use of Technology in Coercive Control

2. Admitting Digital Evidence

3. Skills Building – Mock Admission of Digital Evidence

4. Electronic Evidence in the NYS Courts

.5 Hours

5. Ethical Issues in Electronic Evidence NY Rules

Table of Contents

Evidence in Family Law Matters: Clearing Evidence Hurdles

Part 1

1 ☐ **EVIDENCE IN DOMESTIC VIOLENCE CASES**

How are you going to prove what you need to prove to win your client's case?

2 ☐ **How Do You Prove Your Case?**

- Sources of Evidence
  - ➤ Police records
  - ➤ Medical records
  - ➤ Criminal justice records
  - ➤ Audio/video recordings
  - ➤ Photographs
  - ➤ Writings
  - ➤
-

3 ☐ **How Do You Prove Your Case?**

- Sources of Evidence
  - ➤ "Gifts"
  - ➤ Excited utterances (new DIR)
  - ➤ Party admissions
  - ➤ Experts to explain victim behavior or other dynamics of domestic violence
  - ➤ Fact witnesses

4 ☐ **How Do You Prove Your Case?**

- Sources of Evidence
  - ➤ Weapons
  - ➤ Damaged items
  - ➤ Emails, texts, Facebook posts
  - ➤ Anything else that
    - ❖Can help tell your client's story
    - ❖Can help disprove other side's story
    - ❖You can figure out how to get admitted
-
-

5 ☐ **Laying a Foundation**

- What does that mean??
  - ➤ Relevant to an issue in the case
  - ➤ Material
    - ❖Admissible
    - ❖Non-hearsay or an exception to hearsay

- ❖More probative than prejudicial
- ➢ It is what it purports to be
- ➢ It hasn't been altered or manipulated
- ➢

6 ☐ **What testimony do you need to accomplish this?**

- A witness prepared it or can identify it
- How is it identifiable?
- Is it same or substantially same OR
- It is a fair representation of what it purports to represent (photo or diagram)?

7 ☐ **What testimony do you need to accomplish this?**

- Chain of custody may be important
- Original document, or good reason why not
-
-

8 ☐ **Evidence**

- Remember – for fact-finding hearing, evidence must be material, relevant and competent

- For dispositional hearing, evidence only needs to be material and relevant, so a lot more can come in – shoot for the moon!

9 ☐ **Evidence**

- Know what kinds of evidence you have/need, and think about admissibility and limitations in advance
- Prepare your arguments in advance
- Consider motions *in limine* or notice to admit
- Do your research – don't expect to remember this from law school unless you use it every day

10 ☐ **Danger/Lethality Assessment**

- Now on NYS Domestic Incident Report form
- Also being used in civil courts in NY
  - ➢ Form created by courts and Center for Court Innovation
  - ➢ Provided for judges to guide their decision-making

11 ☐ **Danger/Lethality Assessment**

- Use this to help in drafting petitions
- Talk to your clients about this information
- Look at the guide and make sure the things they're looking for are in the petition, if possible
- Understand context of client's life
- "What does that mean to you?"

12 ☐ **Types of Evidence**

- Testimonial Evidence
  - ➤ Witnesses who saw, heard, felt, smelled, or tasted something at issue in the case
  - ➤ Experts who can render an opinion or educate the finder of fact about something at issue in the case

13 ☐ **Testimonial Evidence – Foundational Issues**

- Relevance
- Witness had ability/opportunity to perceive event testimony pertains to
- Sworn to be truthful
- Expert is qualified to render opinion
-

14 ☐ **Types of Evidence**

- Physical Evidence – some item that was seen, heard, felt, smelled, or tasted
  - ➤ A weapon
  - ➤ A piece of clothing
  - ➤ A "gift"
  - ➤ Any object that is relevant based on the incident in question
  - ➤

15 ☐ **Physical Evidence – Foundational Issues**

- Relevant
- Material
- Witness can identify it
- Item is what it is purported to be
- Same or substantially same as when first perceived
-
-

16 ☐ **Types of Evidence**

- Documentary Evidence – a document that explains or tends to prove or disprove something
  - ➤ Medical records
  - ➤ Police reports
  - ➤ Forensic reports
  - ➤ A printed copy of an email or text
  - ➤

17 ☐ **Documentary Evidence – Foundational Issues**

- Relevant

- Material
- Exceptions to hearsay rule, or why non-hearsay
- Best evidence
  - ➤ For print-outs of emails & texts
  - ➤ For copies of other documents

18 ☐ **Types of Evidence**

- Demonstrative – is not a piece of physical evidence, but can help demonstrate something relevant
  - ➤ Diagram or map of a home or other physical location
  - ➤ Photographs
  - ➤ Charts, timelines, etc.
  - ➤ Limited only by your imagination
  - ➤ Technology presents real opportunities

19 ☐ **Demonstrative Evidence – Foundational Issues**

- Relevant
- Material
- Fair representation of what it's supposed to be a representation of
- Reason it is being used rather than original item

20 ☐ **Types of Evidence**

- Hybrids
  - ➤ Card received by victim
    - ❖Physical evidence OR
    - ❖Documentary evidence
    - ❖Or both at once
  - ➤ Often depends on what you want to use it for

21 ☐ **Voice Recordings**

- Demonstrate that recording equipment was working properly & how recording made
- Witness recognizes voice
- Tape not altered
- Have transcript if using lengthy or unclear tape

22 ☐ **Contact Information**

Ellen C. Schell
General Counsel
NYS Office for the Prevention of Domestic Violence
518-457-5757
ellen.schell@opdv.ny.gov

•

Evidence in Family Law Matters: Clearing Evidence Hurdles

Part 2

NEW YORK STATE | Office for the Prevention of Domestic Violence

EVIDENCE IN DOMESTIC VIOLENCE CASES

How are you going to prove what you need to prove to win your case?

How Do You Prove Your Case?

- Sources of Evidence
  - Police records
  - Medical records
  - Criminal justice records
  - Audio/video recordings
  - Photographs
  - Writings

How Do You Prove Your Case?

- Sources of Evidence
  - "Gifts"
  - Excited utterances (new DIR)
  - Party admissions
  - Experts to explain victim behavior or other dynamics of domestic violence
  - Fact witnesses

How Do You Prove Your Case?

- Sources of Evidence
  - Weapons
  - Damaged items
  - Emails, texts, Facebook posts
  - Anything else that
    - Can help tell your client's story
    - Can help disprove other side's story
    - You can figure out how to get admitted

Laying a Foundation

- What does that mean??
  - Relevant to an issue in the case
  - Material
    - Admissible
    - Non-hearsay or an exception to hearsay
    - More probative than prejudicial
  - It is what it purports to be
  - It hasn't been altered or manipulated

What testimony do you need to accomplish this?

- A witness prepared it or can identify it
- How is it identifiable?
- Is it same or substantially same OR
- It is a fair representation of what it purports to represent (photo or diagram)?

What testimony do you need to accomplish this?

- Chain of custody may be important
- Original document, or good reason why not

Evidence

- Remember – for fact-finding hearing, evidence must be material, relevant and competent
- For dispositional hearing, evidence only needs to be material and relevant, so a lot more can come in – shoot for the moon!

Evidence

- Know what kinds of evidence you have/need, and think about admissibility and limitations in advance
- Prepare your arguments in advance
- Consider motions *in limine* or notice to admit
- Do your research – don't expect to remember this from law school unless you use it every day

Danger/Lethality Assessment

- Now on NYS Domestic Incident Report form
- Also being used in civil courts in NY
  - Form created by courts and Center for Court Innovation
  - Provided for judges to guide their decision-making

Danger/Lethality Assessment

- Use this to help in drafting petitions
- Talk to your clients about this information
- Look at the guide and make sure the things they're looking for are in the petition, if possible
- Understand context of client's life
- "What does that mean to you?"

Types of Evidence

- Testimonial Evidence
  - Witnesses who saw, heard, felt, smelled, or tasted something at issue in the case
  - Experts who can render an opinion or educate the finder of fact about something at issue in the case

Testimonial Evidence – Foundational Issues

- Relevance
- Witness had ability/opportunity to perceive event testimony pertains to
- Sworn to be truthful
- Expert is qualified to render opinion

Types of Evidence

- Physical Evidence – some item that was seen, heard, felt, smelled, or tasted
  - A weapon
  - A piece of clothing
  - A "gift"
  - Any object that is relevant based on the incident in question

Physical Evidence – Foundational Issues

- Relevant
- Material
- Witness can identify it
- Item is what it is purported to be
- Same or substantially same as when first perceived

Types of Evidence

- Documentary Evidence – a document that explains or tends to prove or disprove something
  - Medical records
  - Police reports
  - Forensic reports
  - A printed copy of an email or text

Documentary Evidence – Foundational Issues

- Relevant
- Material
- Exceptions to hearsay rule, or why non-hearsay
- Best evidence
  - For print-outs of emails & texts
  - For copies of other documents

Types of Evidence

- Demonstrative – is not a piece of physical evidence, but can help demonstrate something relevant
  - Diagram or map of a home or other physical location
  - Photographs
  - Charts, timelines, etc.
  - Limited only by your imagination
  - Technology presents real opportunities

Demonstrative Evidence – Foundational Issues

- Relevant
- Material
- Fair representation of what it's supposed to be a representation of
- Reason it is being used rather than original item

Types of Evidence

- Hybrids
  - ➢ Card received by victim
    - ❖ Physical evidence OR
    - ❖ Documentary evidence
    - ❖ Or both at once
  - ➢ Often depends on what you want to use it for

Voice Recordings

- Demonstrate that recording equipment was working properly & how recording made
- Witness recognizes voice
- Tape not altered
- Have transcript if using lengthy or unclear tape

Contact Information

Ellen C. Schell
General Counsel
NYS Office for the Prevention of Domestic Violence
518-457-5757
ellen.schell@opdv.ny.gov

Office for the Prevention of Domestic Violence

8

Evidence in Family Law Matters: Clearing Evidence Hurdles

Part 3

*Technological Abuse:
Electronic Evidence and Ethical Issues

Presented by:

Ian Harris, JD, MA

*Agenda

*Section 1: Electronic Evidence in the NYS Courts

Tech Abuse and Gathering Evidence

Admitting Evidence of Tech Abuse

- Telephonic Technology
- Surveillance Technology
- Computer & Internet Technology
- Subpoenas and Dispositions

Legal Ecosystem

- Federal
- New York State

*Agenda

Section 2: Ethical Issues in Electronic Evidence NY Rules

Legal Ecosystem

- **Ethics**

Ethical Opinions and Standards

Questions

*Goals

This workshop will provide participants with an introduction to:

* **Gathering Evidence of technological issues**
* **Admitting Evidence of technological abuse**
* **How State Civil & Criminal Courts have Dealt with the Admission of Technological Evidence**
* **Federal and State Legislation that can be used to Protect Survivors of Domestic Violence from Technological Abuse**
* **Ethical Issues for Attorneys**

*Importance to Your Work

Why is knowledge of technological abuse important to your job?

* **Increased prevalence of technology**
* **Importance of technology for the lives of survivors of intimate partner violence**
* **Wealth of information available**
* **This information is often deleted/erased**
* **It can be difficult to admit this evidence**
* **Effective dispositions frequently require technological safety provisions**
* ***Technological evidence can greatly decrease the number of cases that need to be litigated***

*What is Technological Abuse?

Cyberstalking
vs.
Technological Abuse

Gathering Evidence

IMPORTANT:

* Maintaining evidence is counter-intuitive

If you get an upsetting email or text, what are you naturally inclined to do?

Types of Technology

* Electronically Stored Information (ESI)
  * Information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software
  * Includes e-mails and attachments, voice mail, instant messaging and other elec. Communications, word processing docs, text files, hard drives, etc…including metadata
* Most data used on behalf of domestic violence survivors will be hard copies of electronically stored documents.

Gathering Tech Abuse Evidence

* Can it prove that the other person is wrong or that your client is right?
* What is the evidence?
* Where is it saved?
* Can client access it? (personally or through another person)
* Do you need it to be certified?

Types of Tech Abuse

* Telephonic Technology
* Surveillance Technology
* Computer & Internet Technology

Telephonic Abuse

- **Constant calls and hang ups or voicemails**
- **Constant Text messages (instant messages)**
- **Spyware**
  - Mspy, Stealthgenie, Mobilespy, etc…
- **Sexting**
- **Spoofing**
  - Spoofcard.com, Telespoof.com, Itellas, *VOIP* etc.

Telephonic Abuse: Other Issues

- **Cordless phone** conversations **can** be monitored
- **Cell phones**—used as a listening device, GPS tracking; **can** be intercepted by scanners
- **Instant messaging** – send threats, intimidate survivor, constant effort to contact survivor
- **Spy phones**—**can** read call logs & emails; **listen** to calls remotely; locater system
- **Blocking Numbers: *** Warning *****

*Surveillance

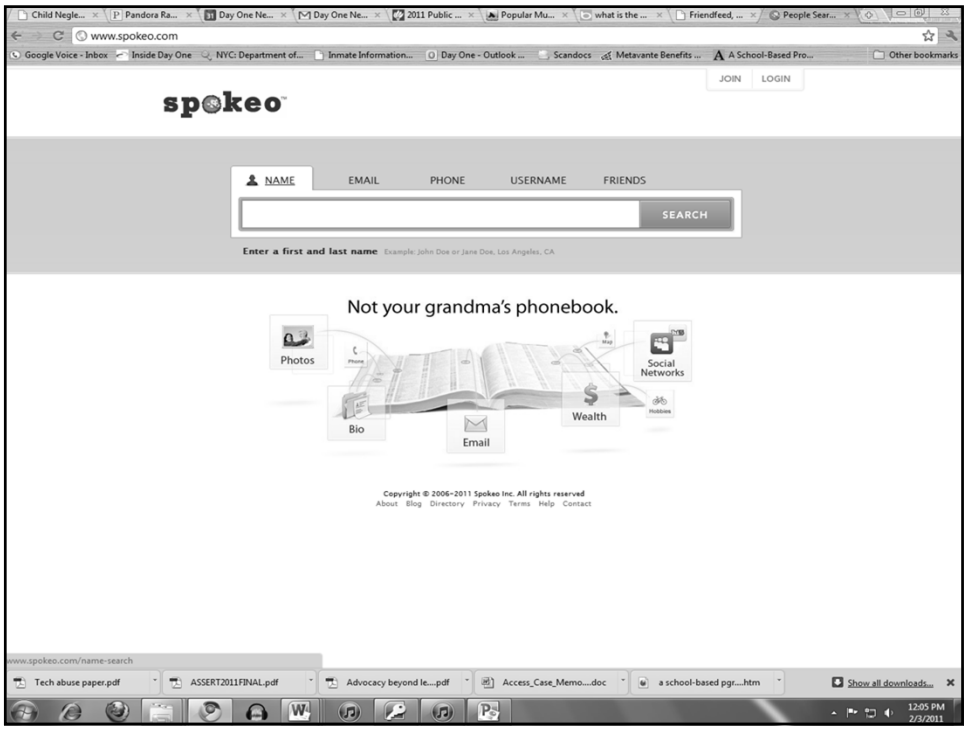
* **GPS** (Global Positioning System) - tracking via cell phones and other devices
* **Cameras** - Webcams, Nannycams, Spycams
* **Social Networking** sites that ask you to check-in (Google Latitude, Yelp, Grindr)

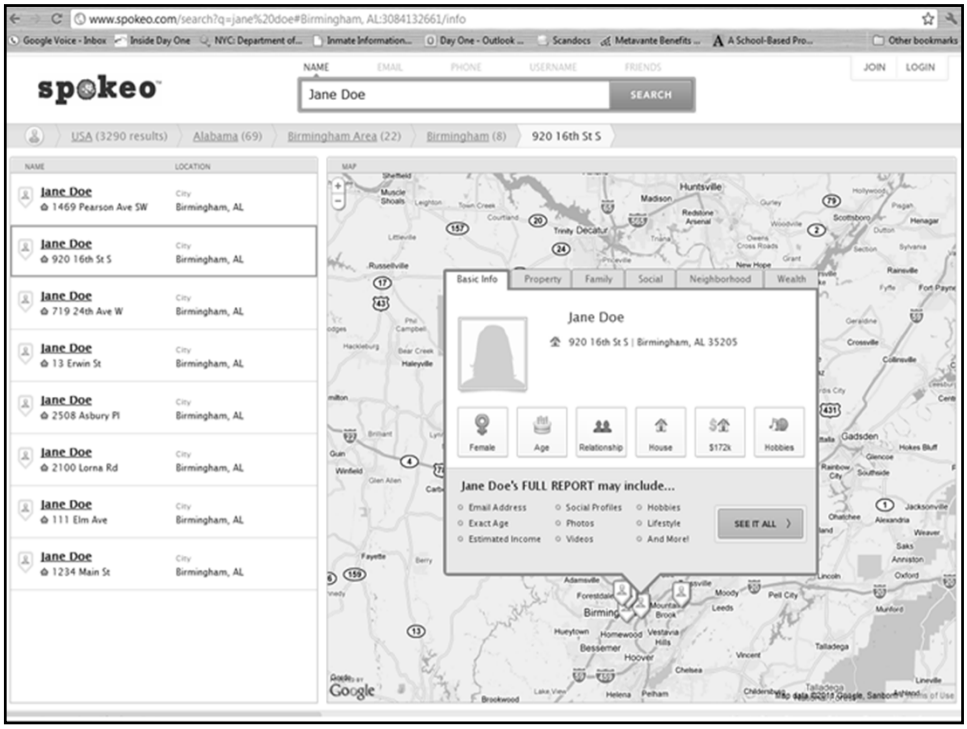
*Computers & Internet Abuse

* **Changing passwords on computers and websites**
* **Gaining access to email accounts**
  * Deleting emails
  * Sending fraudulent emails to coworkers, friends, and/or family;
  * Intercepting email;
* **Creating false virtual profiles on dating or pornographic sites**
  * Posting sexual or pornographic images or text
* **Gaining access w/out consent to social networking sites**
  * Posting rumors
  * Creating discord between friends and family

* Computers & Internet Abuse

* **Formspring.me**
* **Online Investigation**
  * **Intellius,** IRB Search, Accurint, Merlin Information, Tracers Info, TLO, IQ Data, MasterFiles, PublicData
* **Information Aggregation sites:**
  * **Spokeo**
  * **Others: friendfeed, MyLifeBrand, Fuser, hellotxt, MySocial24x7, AlertThingy, twirl, Flock, Profilactic, Xoopit, Socialthing, Iminta, Readr, Onaswarm, Whereisme, Oneswirl, Dipity, Zupme**



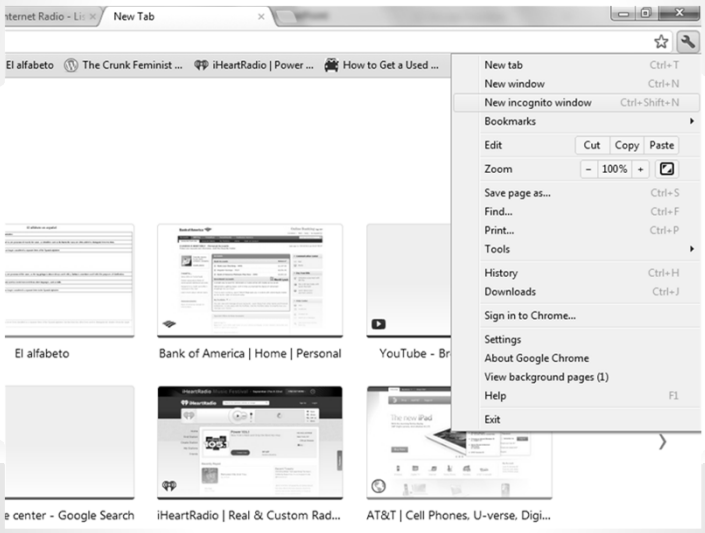


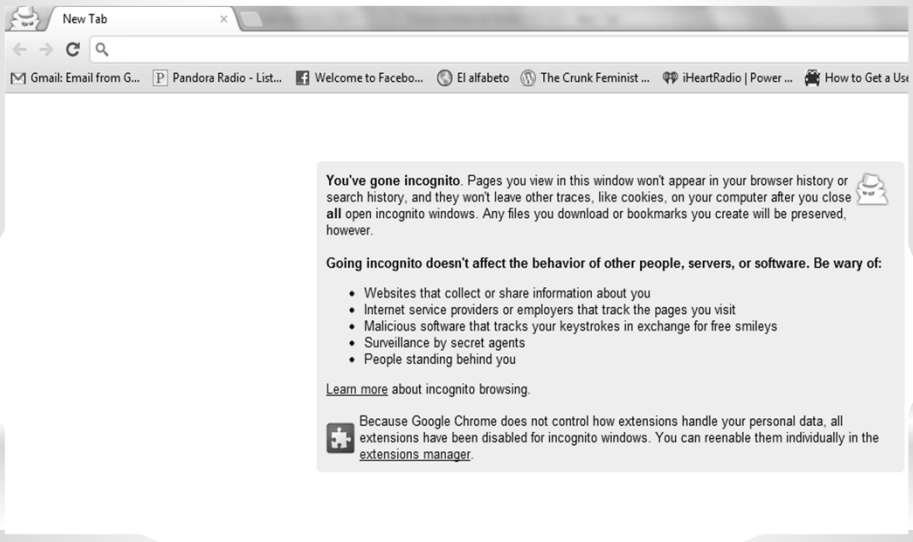
*Computers & Internet

What can you do if somebody is harassing your client with computer & internet technology?

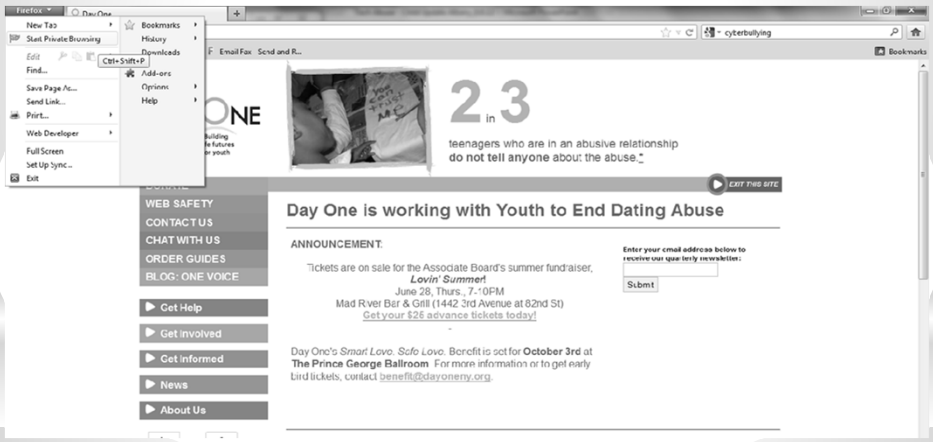
- Do a **Google search** to see what information is available about your clients
- Download Anti-spyware software & Run spyware checks
- Take “Screen shots” or “screen captures” of harassing information on their computers (also on some cell phones & smart phones).
- Print IMs, Text messages, Email messages (with Headers) and Call logs.
- Make sure that your Instant Messenger saves messages.
- Surf the web in “incognito,” “Private,” or “inPrivate” Browsing”

*Google Chrome

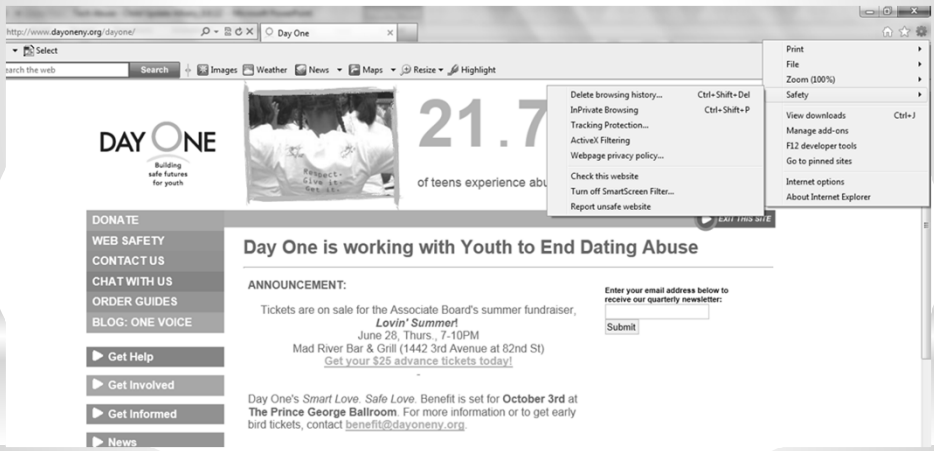




*Mozilla Firefox

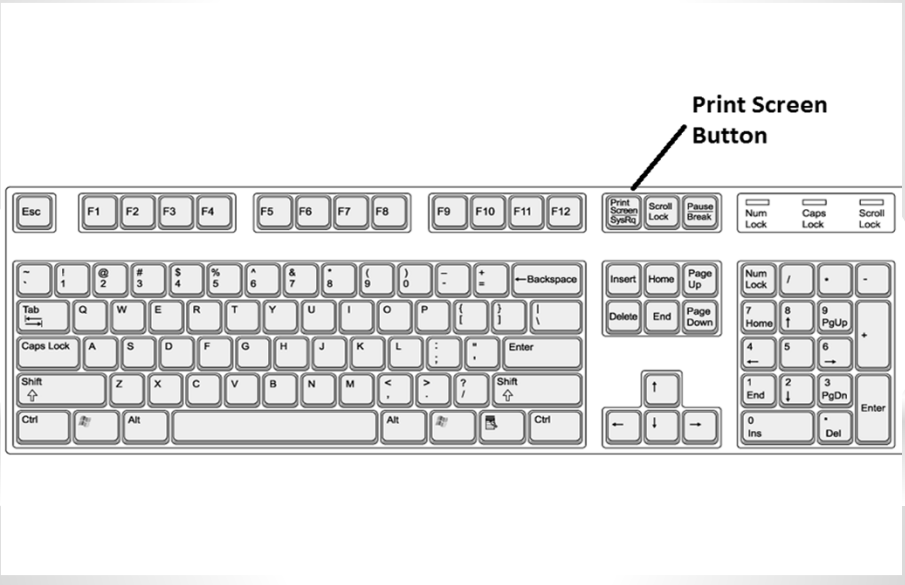


*Internet Explorer



Gathering Evidence

* Encourage survivors to keep a stalking log
  * Log each time a person knows too much
* Save messages (text and audio)
* Take pictures of text messages
* Make sure that Instant Messenger (IM) saves messages
* Take "Screen shots" or "screen captures" of information on a computer (also on smart phones)
* Print IMs, Text messages, Email messages (with headers) and call logs



*Screenshots on a Mac

- Command-Shift-3: Take a screenshot of the screen, and save it as a file on the desktop
- Command-Shift-4, then select an area: Take a screenshot of an area and save it as a file on the desktop
- Command-Shift-4, then space, then click a window: Take a screenshot of a window and save it as a file on the desktop
- Command-Control-Shift-3: Take a screenshot of the screen, and save it to the clipboard
- Command-Control-Shift-4, then select an area: Take a screenshot of an area and save it to the clipboard
- Command-Control-Shift-4, then space, then click a window: Take a screenshot of a window and save it to the clipboard

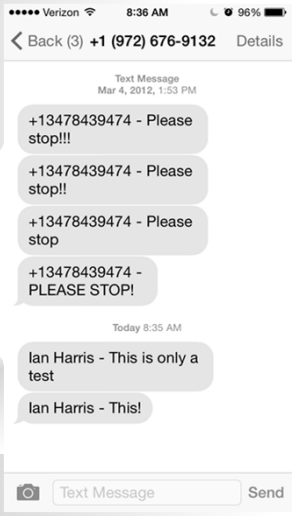
Taking a screen shot

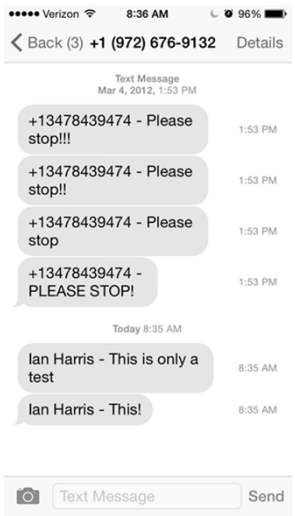
*Gathering evidence

REMEMBER! Print out all of the information:

"From: First name, Last name
CB# xxx-xxx-xxxx
Received:
Feb 4, 09 10:02 am"

*Gathering evidence

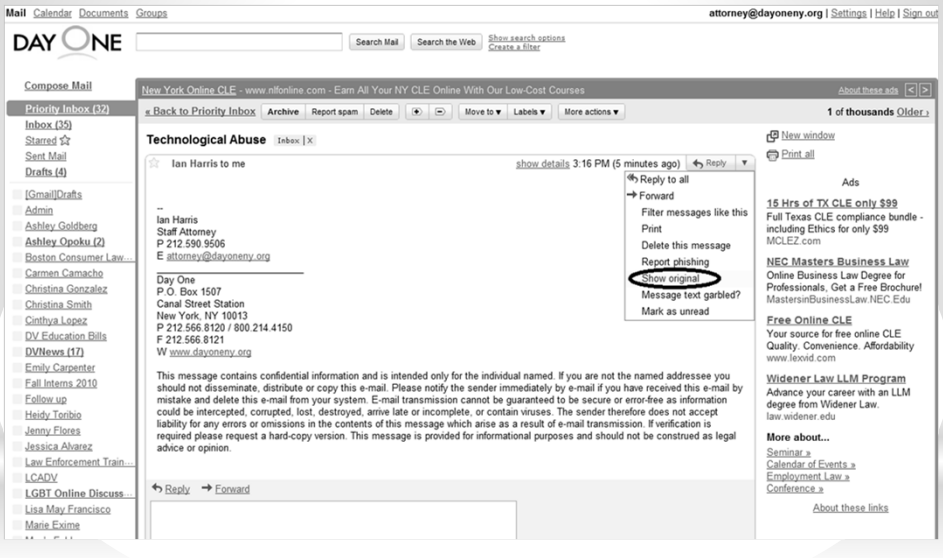


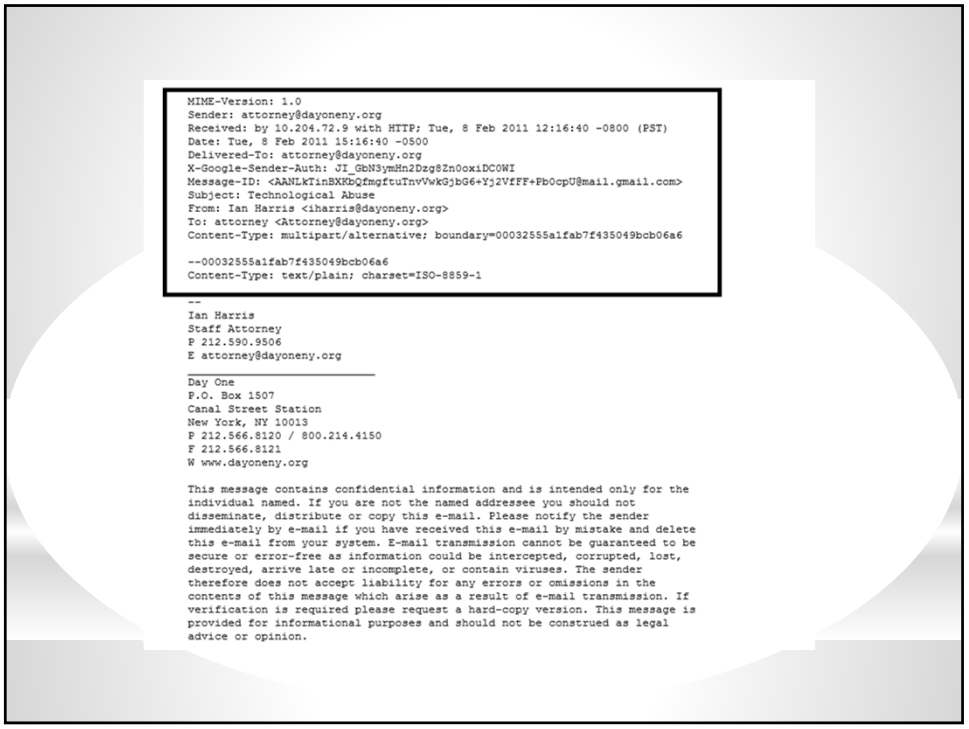


*Gathering evidence: Emails

MAKE SURE TO PRINT EMAILS WITH THE MESSAGE HEADER!

A Message Header is a list of the servers and Internet Protocol (IP) addresses from which a message originated and through which it traveled to reach you.





```
MIME-Version: 1.0
Sender: attorney@dayoneny.org
Received: by 10.204.72.9 with HTTP; Tue, 8 Feb 2011 12:16:40 -0800 (PST)
Date: Tue, 8 Feb 2011 15:16:40 -0500
Delivered-To: attorney@dayoneny.org
X-Google-Sender-Auth: JI_GbN3ymHn2Dzg8Zn0oxiDC0WI
Message-ID: <AANLkTinBXKbQfmgftuTnvVwkGjbG6+Yj2VfFF+Pb0cpU@mail.gmail.com>
Subject: Technological Abuse
From: Ian Harris <iharris@dayoneny.org>
To: attorney <Attorney@dayoneny.org>
Content-Type: multipart/alternative; boundary=00032555a1fab7f435049bcb06a6

--00032555a1fab7f435049bcb06a6
Content-Type: text/plain; charset=ISO-8859-1

--
Ian Harris
Staff Attorney
P 212.590.9506
E attorney@dayoneny.org

Day One
P.O. Box 1507
Canal Street Station
New York, NY 10013
P 212.566.8120 / 800.214.4150
F 212.566.8121
W www.dayoneny.org

This message contains confidential information and is intended only for the
individual named. If you are not the named addressee you should not
disseminate, distribute or copy this e-mail. Please notify the sender
immediately by e-mail if you have received this e-mail by mistake and delete
this e-mail from your system. E-mail transmission cannot be guaranteed to be
secure or error-free as information could be intercepted, corrupted, lost,
destroyed, arrive late or incomplete, or contain viruses. The sender
therefore does not accept liability for any errors or omissions in the
contents of this message which arise as a result of e-mail transmission. If
verification is required please request a hard-copy version. This message is
provided for informational purposes and should not be construed as legal
advice or opinion.
```

*ISSUES WITH HEADERS

* Anonymity
* Spoofing
* Other party does not provide a complete list of IP addresses

*Evidentiary Issues

*Tech Abuse: Evidence and Case Law

*Technology and Evidence: A Primer

*Evidence and Case Law

- Telephonic Technology
- Surveillance Technology
- Computer & Internet Technology
- Subpoenas
- Dispositions

Tech Evidence: Things to Remember

* **Technology may present complicated issues, but the rules are the same**
* *The Good News*: Technology frequently provides evidence where none existed before
* *The Bad News*: Technology, while generally reliable, may allow for anonymous or fake evidence
* Nothing disappears online, but it may be difficult to locate
* Using technology to harass or abuse somebody can have major emotional and physical repercussions

Tech Evidence: The Basics

1. Is evidence **relevant**? (Rule 401)
2. If relevant, is evidence **authentic?** (Rule 901)
3. If offered for substantive truth, is it **hearsay?** (if so, is there an exception?)
4. Is the evidence an **original** *or* **duplicate** under the original writing rule? (is there admissible secondary evidence to prove the content)
5. Does the **probative** value substantially outweigh the danger of unfair prejudice.

*Tech Evidence: Hearsay

Why are the parties seeking to admit the evidence?

1. Admission by Party Opponent
2. Prior Inconsistent Statement
3. Present Sense Impression
4. Etc…

*Tech Evidence: Best Evidence Rule

Rule 1002; CPLR 4539

Most courts "require the production of an original writing where its contents are in dispute and sought to be proven."

What if there is not an "original?"

*Tech Evidence: Best Evidence Rule

Rule 1003; CPLR 4539(b)

"[a] **reproduction** created by any **process which stores** an image of any writing, entry, print or representation and **which does not permit additions, deletions, or changes without leaving a record** of such additions, deletions or changes, when **authenticated by competent testimony or affidavit** which shall include the manner or method by which tampering or degradation of the reproduction is prevented, shall be admissible in evidence as the original."

*Telephonic Evidence: Text Messages

The owner or possessor of a telephone has the "right to be free of unwanted text messages. The brevity of a text message has no impact on the severity of its meaning. A short text message can be more vicious and threatening then a lengthy, convoluted e-mail or letter…"
People v. Pierre, 41 A.D.3d 289, 291, 838 N.Y.S.2d 546, 548-49 (2007)

* **What is a Text message?**
* **Form of Text Message Evidence:**
  - Screenshot or digital photo
  - Phone or Computer
  - Records from Phone or Messaging Company
  - Print out, cut-and-paste, or handwritten transcript

*Telephonic Evidence: Text Messages

Authentication

- **Who can Authenticate?:**
  - Person who saw the message (recipient, sender, or third party)
    - Testify what the message says (screenshot or the actual phone)
    - Testimony of what a deleted message said
  - Phone records (Business Record)

*Telephonic Evidence: Text Messages

Authentication

Cases (Various Jurisdictions):

- **"Authenticity can be shown through the testimony of a participant to the conversation that the document is a fair and accurate representation of the conversation"** United States v. Gagliardi, 506 F.3d 140 [2d Cir.2007];
- A participant to the conversation testified that the **print-out** of the electronic communication was an accurate representation of the exchange and had not been altered in any significant manner]" United States v. Tank, 200 F.3d 627 [9th Cir.2000];
- A **handwritten transcript** of text messages was properly authenticated through testimony from the recipient of the messages, who was also the creator of the transcript. State v. Roseberry, 967 N.E.2d 233 [Ohio 2011];
- **Testimony** from a participant to the conversation was **sufficient**. Jackson v. State, 320 S.W.3d 13 [Arkansas 2009].

* Telephonic Evidence: Text Messages

Other Considerations

* **Authenticity and Reliability**
  - "Court erred in admitting text message from cellular telephone [without] establishing authenticity or reliability of text message [and] permitting jury to access entire contents of cellular telephone. People v. Givans, 45 A.D.3d 1460 (NY Sup Ct. 2007)
  - Failure to authenticate 10 out of 12 text messages was error. Evidence is needed to show not simply that messages came from a particular phone, but that the **alleged author of the messages was the one who actually sent them**. People v. Rodriguez, 128 Nev. Adv.Op 14, 273 P.3d 845 (Sup.Ct., Nev., 2012)
  - **Detective's transcriptions** of text messages on defendant's cell-phone were **not properly authenticated**… prosecution offered no direct proof [from]testimony of recipients or other possible authors of the messages and the message contents did not provide any circumstantial evidence as to authorship; while text messages are unique to the cell-phone from which they were sent, the **owner of the cell-phone does not necessarily have exclusive access to it**. Commonwealth v. Koch, 39 A.3d 996 (Pa.Super.Ct., 2011) [Appeal *granted*, 44 A.3d 1147 (May 2012)]
* **Anonymous and Fraudulent Text Messages**

* Telephonic Evidence: Phone Calls

"An individual has a substantial privacy interest in his or her telephone...the device is easily conceptualized as the functional equivalent of the mailbox." The owner or possessor of the telephone has the "right to be free of unwanted telephone calls..."
People v. Shack, 536, 634 N.Y.S.2d 660, 658 N.E.2d 706

* **Form of Phone Call Evidence:**
  - Screenshot or digital photo of call log
  - Phone (call logs)
  - **Records from Phone Company**
  - Print out, cut-and-paste, or handwritten transcript
  - *Recordings of messages left on voicemail*

* Telephonic Evidence: Phone Records

* **Form of Phone Record Evidence?**
  - Business Record
  - Print out from litigants
* **What do Phone Records Include?**
  - Caller/Texter # and time of call/text
  - Some Companies may have text content
* **Authentication?**
  - Business Records
  - Testimony from account owner
  - Testimony from third party witness
  - Consent of parties

* Telephonic Evidence: Phone Records

Other Considerations: Subpoenas

* **Opposing Party**
  - The third department noted that a party in a matrimonial action **could not subpoena** telephone logs and AOL instant messages chat logs without a showing that they are **necessary for custody determination**. Bill S. v Marilyn S., 8 Misc.3d 1013(A) (2005).
* **Nonparty**
  - The third department **declined to sign a subpoena** for **third party phone records**, noting that parties in a matrimonial action are not entitled to "disclosure against non-parties without **'showing special circumstances**, i.e., that the information sought to be discovered is material and necessary and cannot be discovered from other sources'" Bill S. v Marilyn S., 8 Misc.3d 1013(A) (2005).

*Surveillance Evidence

Recording & Videographic Evidence

* **What is Surveillance?**
  * **Videos**
  * Audio recordings
  * GPS and other tracking records
* **Form of Surveillance Evidence:**
  - Video and audio recordings (on phones, other devices, and other storage formats)
  - Print out of GPS and tracking information

*Surveillance Evidence

Authenticating Videographic Evidence

* **Who can Authenticate?**
  - Testimony of any person present when the activity occurred
  - Even without the person testifying, the remaining foundational elements have sufficient probative value to verify the film

*Surveillance Evidence

Authenticating Videographic Evidence

* **Foundation**** New York courts have applied the standard for determining admissibility of photographs to evaluate the admissibility of video evidence.
  - Identity of subject matter;
  - Qualifications of operator who filmed the video or one who was a participant in the recording;
  - Authenticity and accuracy-portrayal of a true, fair and accurate representation of events, people and/or scene depicted;
  - Type and quality of film and video equipment;
  - Manner of developing;
  - Continuity of possession;
  - Explanation of distortions or changes or editing; and
  - Technical imperfections.

***People v Higgins, 392 N.Y.S.2d 800 [N.Y. Sup.Ct.1977]*

*Surveillance Evidence

Case Law

* Testimonial evidence must come from a "**witness to the recorded events**, or of an **operator** or **installer** or **maintainer** of the equipment" or "by the photographer, or technician or engineer, or by any one who observed the events depicted" who can testify that the videotape "**accurately represents the subject matter depicted.**" *People v. Patterson 93 N.Y.2d 80 [N.Y. 1999]*;
* Videographic evidence is only admissible if it is a **true, fair, and accurate portrayal** of events, people, and the scene depicted. *City v. Prophete 544 N.Y.S.2d 411 [N.Y. Civ.Ct. 1989].*

* Surveillance Evidence

Case Law

* A videotape is **true, authentic, and accurate evidence** if, among other indicators, the tape is filmed with quality video equipment and it is ***without distortion or deletion***. *People v. Curcio 645 N.Y.S.2d 750 [N.Y. Sup.Ct. 1996].*
* Skips or deletions must not be so substantial as to render the whole video **untrustworthy**. *People v. Gucciardo 355 N.Y.S.2d 300 [N.Y. Sup.Ct 1974].*
* Plaintiff's wedding video was relevant to claims that she could no longer engage in activities such as **running or horseback riding**, due to permanent injuries. Sgambelluri v. Recinos, 192 Misc 2d 777 (S. Ct., Nass. Cty.)

* Computer Evidence: E-Mail Messages

* **Anatomy of an Email Message**
  - Header (Sender, Recipient, IP Addresses)
  - Body
  - Signature
* **Forms of Email Message Evidence:**
  - Screenshot or digital photo
  - Phone/Computer
  - Records from Email Company
  - Print out, cut-and-paste, or handwritten transcript

* Computer Evidence: E-Mail Messages

Authentication

* **Who can Authenticate?**
  - Person who saw the message (recipient, sender, or third party)
    - Testify what the message said and where it came from (screenshot or the actual phone/computer)
    - Testimony of what a deleted message said
  - Email records (Business Record)

* **How to Authenticate:**
  - Proof that the email came from the alleged sender
    - Derived from an account available to or connected to the alleged sender
    - Alleged sender is responsible for the email being sent (Intentionally sent the message to the recipient, intentionally used a third party, and/or failed to act)

* **Issues with Authentication:**
  - Emails can be sent anonymously
  - Emails can be "spoofed"

* Computer Evidence: E-Mail Messages

Other Considerations

* **Retrieval of email messages from a person's email account that party had access to is not considered "eavesdropping evidence" and therefore not subject to exclusion under CPLR 4506(1).** Gurevich v Gurevich, 24 Misc.3d 808 (2009)
* **Violation of no contact Order of Protection that Respondent knew or intended that, by sending the e-mail to the Petitioner's family, it would reach the Petitioner.** Matter of Jennifer G. v Benjamin H., 84 A.D.3d 1433 (2011); see also Matter of Duane H. v Tina J., 66 AD3d 1148, 1149 [2009].
* **Email messages sent by computers, cell phones and/or other devices items can constitute aggravated harassment in the second.** Matter of Julie G. v Yu-Jen G., 81 A.D.3d 1079 (2011); M.G. v. C.G., 19 Misc.3d 1125(A) (2008).

* Computer Evidence: E-Mail Messages

Other Considerations

* **Respondent has a duty to ensure that he did not send Petitioner any e-mail messages, even through mass mailings.** Odden v. Rath, 730 N.W.2d 590 (2007)
* **Wife failed to demonstrate that husband was responsible for sending three threatening e-mail messages where the first message indicated that it came from wife's former (shared) account, the second originated from previously unidentified address, and the third was routed through wife's sister and only indicated that original message came from person by wife's name**. Smith v. Smith, 24 A.D.3d 822 (2005).

* Computer Evidence: Social Networking

* **Forms of Social Networking Evidence:**
  - Screenshot or digital photo
  - Phone/Computer
  - Records from Social Networking Company
  - Print out, cut-and-paste, or handwritten transcript

* Computer Evidence: Social Networking

Authentication

* **Who can Authenticate?**
  - Person who saw the message (recipient, sender, or third party)
    - Testify what the message said and where it came from (screenshot or the actual phone/computer)
    - Testimony of what a deleted message said
  - Records from Social Network Company (Business Record)

* **How to Authenticate:**
  - Proof that the posting/information came from the alleged sender
    - Derived from an account available to or connected to the alleged sender
    - Alleged sender is responsible for the information being sent (Intentionally sent the message to the recipient, intentionally used a third party, or failed to act)

* **Issues with Authentication:**
  - Posting can be sent anonymously
  - Postings can be "spoofed"
  - It is unclear who owns the information

* Computer Evidence: Social Networking

Other Considerations

* **Who Owns Social Networking Information?**
  Twitter had to disclose all non-content information and content information for Defendant. Defendant had no proprietary interest in the user information on his Twitter account and lacked standing to quash the subpoena. **People v. Harris 2012 N.Y. Slip Op. 22175.**
* **Discovery of Social Networking Accounts Permitted**
  Discovery of plaintiff's MySpace and Facebook accounts was material and relevant to plaintiff's claim that she could no longer participate in certain activities as a result of injuries. **Romano v. Steelcase Inc., 30 Misc 3d 426 (S. Ct. Suff. Cty.)**
* **Printout of Messages Admissible**
  Facebook message admitted into evidence showing that wife did not post pictures because they would hurt her legal claim. **B.M. v D.M., 31 Misc.3d 1211(A) (2011)**

Computer Evidence: Social Networking

Other Considerations

* **Libel and Defamation**
  Postings not libel where the postings were made on a **"secret" Facebook group, which has no public content and does not appear on a Facebook member's profile.** "Reasonable reader, given the overall context of the posts, simply would not believe that the posts are true." **Finkel v Dauber, 29 Misc.3d 325 (Nassau Sup. Ct. 2010)**
* **The Ability to Alter Photographs May Limit Admissibility**
  Defendant was not allowed to introduce pictures from MySpace in order to cross examine witnesses about their alleged gang membership "In light of the ability to "photoshop," edit photographs on the computer, and defendant could not authenticate the photographs." **People v Lenihan, 30 Misc.3d 289 (Queens Sup. Ct. 2010)**
* **Proof of Intentional Harassment**
  18-year-old defendant could not be charged with aggravated harassment (Penal Law § 240.30 [1]) for having merely sent messages to the 14-year-old complainant through a social networking Web site expressing his unrequited love for her, in the absence of any allegation that the messages were intended to threaten, incite alarm or harass." **People v Rodriguez, 19 Misc.3d 830, 860 N.Y.S.2d 859 (N.Y. City Crim. Ct. 2008)**

Computer Evidence: Websites

Other Considerations

* **Using a Website to Communicate through 3rd Party**
  Defendant and a co-worker created a website containing suggestive photographs and words, and listing complainant's address and telephone numbers with a request that people contact her. She was called twice at work. Defendant's actions constituted criminal contempt and aggravated harassment in the second degree. A defendant is not exculpated because he, instead of placing the phone call to his victim himself, used others to do so. **People v Kochanowski, 186 Misc.2d 441 (2000)**
* **Threats on Public Website = Aggravated Harassment**
  Message on a computer Internet newsgroup which stated "Please kill Police Lt. Steven Biegel, all other NYPD cops, and all of their adult relatives and friends" was aggravated harassment where the officer felt scared. **People v Munn, 179 Misc.2d 903 (1999)**

* Computer Evidence: Orders of Protection

* **Friend Request Is a Violation**
  * People v. Fernino, 19 Misc. 3d 290, 851 N.Y.S.2d 339 (City Crim. Ct. 2008) (myspace.com)
* **Posting on Craigslist is a Violation**
  Criminal contempt found where defendant, in addition to sending victim several violent emails, also posted on Craigslist the victim's name, address, license plate number, place of employment, make and model of her car and false allegations about her illegal immigrant status. People v. Phelan, 82 A.D.3d 1279, 918 N.Y.S.2d 608 (3d Dep't 2011), leave to appeal denied, 17 N.Y.3d 799, 929 N.Y.S.2d 107, 952 N.E.2d 1102 (2011)
* **Contacting Facebook friends of Petitioner Not a Violation**
  People v. Welte, 31 Misc. 3d 867, 920 N.Y.S.2d 627 (J. Ct. 2011)

* Computer Evidence: Computer Memory

* **Computer Memory is Akin to a File Cabinet**
  "Plaintiff did not act illegally by removing the 'family' computer from the marital residence. Plaintiff wife is entitled to access to information concerning defendant husband's finances and personal business records stored in a laptop computer owned by defendant's employer but kept by defendant in his home…Computer memory is akin to a file cabinet and plaintiff clearly could have access to the contents of a file cabinet left in the marital residence." **Byrne v Byrne, 168 Misc.2d 321 (1996)**
* **May Have Access to Hard Drive of Family Computer**
  Wife's access to material downloaded and saved to the hard drive of the computer found by the wife in the trunk of her husband's car was not the result of an intercepted communication and does not constitute a violation of Penal Law § 250.05. **Moore v Moore (NYLJ, Aug. 14, 2008, at 26, col 1 [Sup Ct, NY County]). See also Boudakian v Boudakian (NYLJ, Dec. 26, 2008, at 27, col 3 [Sup Ct, Queens County 2008]) and Gurevich v Gurevich, 24 Misc.3d 808 (2009).**
* **Access Should Not be Unrestricted**
  Wife's allegations that defendant husband concealed and misrepresented his income and assets were insufficient to justify the *unrestricted* turnover of defendant's office computer hard disk drive. **Schreiber v Schreiber, 29 Misc.3d 171 (2010)**

* Tech Evidence: Subpoenas

Considerations

* **Subpoenas Regularly Signed by Judges for Tech Evidence**
  - Identity of account holder and communications obtained by service of a subpoena on the Internet service provider." People v Foley, 257 A.D.2d 243 (1999).
  - Family offense proceeding alleging that father sent vulgar messages to mother, court approved subpoena directing Yahoo!, to disclose only information identifying father as holder of the e-mail account and the contents of e-mail messages sent from that account to the mother's e-mail account during a designated time-frame. ***Matter of D.M. v. J.E.M.,* 873 N.Y.S.2d 447 (Fam. Ct., Orange Co., 2009)**
  - Subpoena of e-mails, telephone logs and three years of AOL instant messages chat logs to establish divorce grounds rejected as overbroad; court noted that more latitude is afforded to discovery regarding financials, as compared to grounds) ***Matter of Bill S. v. Marilyn S.*, 8 Misc.3d 1013(A) (Sup.Ct., Nassau Co., 2005)**
* **Subpoenas May be Expensive**
  - there are no domestic violence exceptions.
  - Many telephone companies are similarly expensive.

* Tech Evidence: Subpoenas

Considerations

* **Limited response to Civil Subpoenas**
  - Most tech companies only respond to valid **law enforcement** subpoenas, unless:
    - The information is indispensible to the case
    - Info not in the Party's possession, Personal service of valid Federal, California, or California domesticated subpoena
    - Must give notice to the individual's impacted and other party.

*Tech Evidence: Orders of Protection

Sample Language

- Observe such other conditions as are necessary to further the purposes of protection: respondent not to post any references to the petitioner on any internet site.
- "Refrain from communication or any other contact by mail, telephone, e-mail, voice-mail, or other electronic or any other means with _____ or through social network whether directly or through third parties. Respondent must refrain from disseminating, posting or distributing any sexually explicit photos, tapes or online recordings involving the Petitioner."

*Tech Evidence: Orders of Protection

Sample Language

- "No contact with petitioner through any method of communication including but not limited to cell phone, text message, email, regular mail correspondence, any social networking site such as Facebook, AIM "chat," etc. or third person contact;
- "Observe such other conditions as are necessary to further the purposes of protection: Neither party to contact each other on Facebook or any other internet based social network. Both parties are to remove each other as "contacts/friends" from any internet based social network forthwith." No 3rd party contact.

* Tech Evidence: Juvenile Delinquency

* Based on posting of a video of an assault on MySpace in violation of condition of interim release, the court included a prohibition on computer use other than educational purposes. Matter of Ashley D., 55 A.D.3d 605 (2008)

* Tech Evidence: Jurisdiction

* **Phone Calls & Letters Enough to Establish Personal Jurisdiction**
  - While "random, fortuitous, or attenuate contacts are not sufficient" to establish 'minimum contacts' under a long-arm statute, courts must consider the "nature and quality of actions." The abusive actions taken was not like circumstances surrounding business transactions by mail and/or phone and because the acts repeatedly had their effect in another state, that was sufficient to establish minimum contacts. Beckers v. Seck 14 S.W.3d 139 (2000)
* **Purposeful Injurious Actions Can Establish Personal Jurisdiction**
  - "A forum may assert specific jurisdiction over a non-resident defendant where an alleged injury arises out of or relates to actions by the defendant himself that are purposefully directed toward forum residents, and where jurisdiction would not otherwise offend 'fair play and substantial justice.'" Burger King v. Rudezewicz 471 U.S. 462 (1985)

*Legal Ecosystem

*Legal Ecosystem

* **New York State Law**
  - Penal Law
  - Evidentiary Law (New York and Federal)

* **Federal Law**
  - The Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2501)
    - Stored Communications Act (SCA) (18 U.S.C. §§ 2701–2712)
    - The Wiretap Act (18 U.S.C. §§ 2510-2522)
  - Federal Stalking Law (Interstate Communications) (18 USC § 875)
  - Obscene or harassing telephone calls (47 USC § 223)
  - Violence Against Women Act (VAWA)
    - Interstate domestic violence (18 USCS § 2261)
    - Stalking (18 USCS § 2261A)

*New York State: Penal Law, Tech

- **Eavesdropping** (P.L. §250.05)
- **Unauthorized Use of a Computer** (P.L. *§156.05*)
- **Computer Trespass** (P.L. *§156.10*)
- **Computer Tampering (4th – 1st degree)** *(*P.L. *§156.20 - §156.27*)
- **Stalking** (P.L. §120.45)
- **Unlawful Surveillance** (P.L. §250.40)
- **Tampering with private communications** (P.L. *§ 250.25*)
- **Dissemination of an Unlawful Surveillance Image** (P.L. *§250.55*)
- **Disseminating Indecent Material to Minors in the first and second degree** (P.L. *§235.21 -§235.22*)
- **Criminal Mischief in the fourth degree** (P.L. *§145.00*)

*New York State: Penal Law, General

- ***Aggravated Harassment in the Second Degree*** (P.L. *§240.30*)
- **Harassment** (P.L. *§240.25*)
- **Menacing** (P.L. §*120.14*)
- **Disorderly Conduct** (P.L. *§240.20*)

* Federal: Electronic Communications Privacy Act (ECPA)

18 USC § 2501

* **Purpose:**
  Makes it **unlawful** for a person to **intentionally intercept** any wire, oral, or electronic communication, or to **use** or **disclose** any wire, oral, or electronic communication that has been intentionally intercepted.

* **Penalties:**
  Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted

* **NOTE**: May be Permissible to intercept any wire, oral, or electronic communication if: 1) party to the communication or 2) one of the parties to the communication gives prior consent.

* Federal: Stored Communications Act (SCA)

18 USC Chapter 121 §§ 2701–2712

* **Purpose:**
  Makes it unlawful to **intentionally access**, without authorization, an electronic communication service or… **intentionally exceed an authorization** to access that facility. The Law also describes the conditions under which the government is able to compel disclosure of "customer or subscriber" content and non-content information for each of these types of service (§ 2703). Applies to:
  - "**Electronic communication services**" (any service which provides to users the ability to send or receive wire or electronic communications) and
  - "**Remote computing services**" (Any service that provides the public with computer storage or processing services by means of an electronic communications system).

* **Penalties:**
  - Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted

* Federal: The Wiretap Act

18 U.S.C. §§ 2510-2522

* **Purpose:**
  Prohibits the intentional interception, use, or disclosure of wire and electronic communications. Bars third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.
* **Penalties:**
  Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted
* **NOTE**:
  There are statutory exceptions, such as a properly secured warrant for a wiretap.

* Federal: Federal Stalking Law

18 U.S.C. § 875

* **Purpose:**
  875(C) **Prohibits transmitting** in interstate or foreign commerce any communication containing any **threat to kidnap** any person or any **threat to injure** the person of another.
* **Penalties:**
  Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted.

* Federal: Obscene or harassing telephone calls

47 U.S.C. § 223

* **Purpose:**
  Makes it a crime to use a telephone or telecommunications device to annoy, abuse, harass, or threaten.
* **Penalties:**
  Criminal Penalty: fine or imprisonment of not more than two years, or both. (Misdemeanor)
* **NOTE**:
  Broader than federal stalking law, because it covers threats and harassment.

* Federal: Violence Against Women Act (VAWA)

18 U.S.C. § 2261 – Interstate Domestic Violence

* **Purpose:**
  A. Prohibits travel with the intent to kill, injure, harass, or intimidate a spouse, intimate partner, or dating partner, where in the course of or as a result of such travel or presence, commits or attempts to commit a crime of violence against that spouse, intimate partner, or dating partner.

  B. Prohibits causing a spouse, intimate partner, or dating partner to travel by force, coercion, duress, or fraud, and who, in the course of, as a result of, or to facilitate such conduct or travel, commits or attempts to commit a crime of violence against that spouse, intimate partner, or dating partner
* **Penalties:**
  Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted.

* Federal: Violence Against Women Act (VAWA)

18 U.S.C. § 2261A and b

* **Purpose:** § 2261A (Stalking)
  Prohibits the use of "mail, **any interactive computer service**, or any facility of interstate or foreign commerce to engage in a course of **conduct that causes** substantial **emotional distress** to that person or places that person in **reasonable fear of the death** of, or **serious bodily injury**."
* **Purpose:** 18 USC § 2261(b)
  Increased penalties for those who stalk while subject to a **civil protection or restraining order.**

*Ethics!

* **Evidence: Civil Practice Law and Rules *(*CPLR)**
* **Ethics Rulings and Ethical Standards**

* New York State: Evidence

* **Eavesdropping evidence** (CPLR §4506 (1))
  - Eavesdropping evidence obtained in violation of Penal Law § 250.05 may not be received in evidence
* **Privileged communications; electronic communication thereof** (CPLR §4548)
  - No privileged communication shall lose its privileged character for the sole reason that it is communicated by electronic means
* **Business records** (CPLR §4518)
  - An electronic record shall be admissible in a tangible exhibit that is a true and accurate representation of such electronic record.
* **Best Evidence Rule** CPLR 4539(b):

* Ethical Standards and Tech

* Ethics Decisions: Social Network

* **Attorneys May advise Clients to Take Offensive Material off Social Networks**

  However, a lawyer may not advise a client to destroy evidence. *NYCLA Comm. On Professional Ethics Formal Opinion #745: (July 2, 2013)*

  - **Rule 3.4 – *shall not suppress evidence; use false evidence; create or preserve false evidence***

* Ethics Decisions: Social Network

* **Obtaining Evidence From Social Networking Websites**

  A lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent. *The Assoc. of the Bar of the City of NY Committee on Professional and Judicial Ethics Formal Opinion 2010-2.*

  - **Rule 4.2 – *Shall not communicate with rep'd party***
  - **Rule 4.4 – *a. no methods of gathering evidence that violate rights b. Must notify sender of inadvertent sharing of information***
  - **Rule 4.3 – *Shall not imply disinterest with unrep'd person***

* Ethics Decisions: Social Network

* **Lawyer's Access to Public Pages of Another Party's Social Networking Site for the Purpose of Gathering Information in Pending Litigation**

  A lawyer in pending litigation may access the public pages of another party's social networking website (such as Facebook) for the purpose of obtaining possible impeachment material for use in the litigation. *NYS Bar Association Comm. on Professional Ethics Opinion 843: (9/10/2010)*

  - **Rule 4.2 – *Shall not communicate with rep'd party***
  - **Rule 4.4 – *a. no methods of gathering evidence that violate rights***
  - **Rule 4.3 – *Shall not imply disinterest with unrep'd person***

* Ethics Decisions: Jury

* **Jury Research and Social Media**

  Attorneys may use social media websites for juror research. No communication may occur between the lawyer and the juror. Attorneys may not research jurors if the result of the research is that the juror will receive a communication. Bar of the City of NY; *Formal Opinion 2012-2*

  - **Rule 3.5 – *Shall not communicate with a juror***
  - **Rule 3.6 – *Shall not make extrajudicial statement, that will be reasonably disseminated, that is substantially likely to cause material prejudice***

* Ethics Decisions: Jury

* **Lawyer Investigation of Juror Internet and Social Networking Postings During Conduct of Trial**

  A lawyer may undertake a pretrial or trial search. Must not "friend," email, send tweets to jurors or otherwise communicate with the juror, or act in any way by which the juror becomes aware of the monitoring. *NYCLA Comm. On Professional Ethics Formal Opinion #743: (May 11')*

  - **Rule 3.5 – *Shall not communicate with a juror***
  - **Rule 3.6 – *Shall not make extrajudicial statement, that will be reasonably disseminated, that is substantially likely to cause material prejudice***

* Ethics Decisions: Confidentiality

* **Using email to communicate with clients**

  A lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information, unless there is a heightened risk of interception. Must select a more secure means of communication if information is of extraordinarily sensitive nature and therefore reasonable to use only a means of communication that is completely under the lawyer's control. *Must stay abreast of evolving tech. N.Y. State #709 (1998)*

  - **Rule 1.6 – *Shall not knowingly reveal confidential info***

* Ethics Decisions: Confidentiality

* **Searching Inadvertently Sent Metadata in Opposing Counsel's Electronic Documents**

  A lawyer is ethically obligated to avoid searching metadata of electronic documents that appear to contain inadvertently produced metadata. *NYCLA Opinion #738*

  - **Rule 4.4 – *a. no methods of gathering evidence that violate rights b. Must notify sender of inadvertent sharing of information***

* Ethics Decisions: Confidentiality

* **Confidentiality; Remote Access to Firm's Electronic Files**

  A law firm may use a system that allows its lawyers to access the firm's document system remotely, as long as it takes reasonable steps to ensure that confidentiality of information is maintained. *NYS Bar Opinion #1019*

* **Confidentiality; Use of Cloud Storage for Purposes of a Transaction**

  A lawyer may post and share documents using a "cloud" data storage tool if the technology employed provides reasonable protection to confidential client information OR if the lawyer obtains informed consent from the client after advising the client of the relevant risks. *NYS Bar Opinion #1020*

  - **Rule 1.6 – *Shall not knowingly reveal confidential info***

*Ethical Standards and Tech

* **Rule 3.3 a3 –** ***Shall not knowingly use false evidence***
* **Rule 5.3 –** ***all rules also apply to non-lawyers that you work with***

*RESOURCES

* Resources for Survivors

* **Safe Shepherd - www.safeshepherd.com/advocates**
  * Free premium service for stalking victims
* **Reputation.com**
  * Free service for domestic violence victims
* **NNEDV - The SafetyNet Project - www.nnedv.org**
  * Survivors & Technology: An Interactive Safety Planning Tool
* **That's Not Cool - www.Thatsnotcool.com**
* **A Thin Line - www.Athinline.org**

* Resources for Law Enforcement

* Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, January 2007
* Electronic Crime Scene Investigation: A Guide for First Responders, April 2008
* Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, November 2009
* Investigations Involving the Internet and Computer Networks, January 2007
* Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April 2004

Available at http://victimsofcrime.org/src/resources/for-practitioners#cjs

*Use of Technology to Stalk

* Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, January 2007
* Electronic Crime Scene Investigation: A Guide for First Responders, April 2008
* Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, November 2009
* Investigations Involving the Internet and Computer Networks, January 2007
* Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April 2004

Available at http://victimsofcrime.org/src/resources/for-practitioners#cjs

*Questions?

Evidence in Family Law Matters: Clearing Evidence Hurdles

Biographies

Ellen C Schell

Ellen C Schell is Counsel for the NYS Office for the Prevention of Domestic Violence. Previously, she was Counsel to The Legal Project, and provided training and technical assistance to civilian attorneys and advocates working with military-related survivors of intimate partner violence. From 2006 – 2009, Ellen was an Assistant District Attorney in Essex County, New York, where she had primary responsibility for prosecution of domestic violence, stalking, and sexual assault cases. Ellen was also Legal Director at The Legal Project from 2001 until 2006, providing civil legal services to survivors of sexual assault, and supervising other legal services provided by the organization. Ellen graduated from Albany Law School *magna cum laude* in 1993. Prior to law school, she worked in organizations providing direct assistance to survivors of sexual assault and domestic violence.

Ian Harris

Ian Harris is the Director of the Family Law/Domestic Violence Unit at Staten Island Legal Services (SILS) in New York City. Before joining SILS, Ianrepresented survivors of intimate partner abuse in family, matrimonial, and immigration law matters as a staff attorney with the New York Legal Assistance Group's (NYLAG) Matrimonial & Family Law Unit and at Day One, a NYC-based organization that focuses on young survivors of intimate partner abuse. Ian has taught as an Adjunct Professor of Sociology and Gender Studies at Wagner College. He is the Chair of the New York City Bar Association Domestic Violence Committee and the secretary of the Lawyer's Committee Against Domestic Violence. He received his JD from the American University Washington College of Law and an MA from the American University School of International Service.

Katherine Woodhouse McGerald

Katherine Woodhouse McGerald has provided legal representation to hundreds of clients and survivors for over 15 years with a focus on providing holistic legal services to survivors of domestic violence, intimate partner violence, sexual assault, harassment based on gender or gender identity, and stalking. Her areas of expertise include intimate partner violence litigation, sexual assault litigation, family court proceedings, and trial advocacy.

She worked as an assistant district attorney at The New York County DA's Office, as a staff attorney at The Pace Women's Justice Center, and a senior staff attorney at Legal Services of the Hudson Valley. While at the Manhattan DA's Office, she was a member of the Domestic Violence Unit and Sex Crimes Unit. At the Women's Justice Center Katherine supervised attorneys and law students in the Family Court Externship. As a Senior Staff Attorney at Legal Services of the Hudson Valley, she provided direct legal services and advocacy to victims of intimate partner violence, sexual assault, and stalking in Family Court, Supreme Court, City/Town Courts, and meetings in family offense, custody, child support, housing, public benefits, title ix, divorce, and immigration matters in Orange, Sullivan and Dutchess Counties.

Katherine graduated from Pace University School of Law where she participated in the Prosecution of Domestic Violence Clinic and started the Family Court Externship whereby law students represented victims of domestic violence under the supervision of an attorney for the ex-parte family offense proceeding.

Technological Abuse:
Electronic Evidence and Ethical Issues

Index of Materials*

Representing the Legal Services Client: Ethical Issues in Electronic Evidence Under the New York Rules

Index of Materials*

Ethical Opinions:

1. NYCLA Committee on Professional Ethics; Opinion 738 – Searching Inadvertently sent metadata in opposing counsel's electronic documents
2. NYCLA Committee on Professional Ethics; Opinion 743 – Lawyer investigation of juror internet and social networking postings during conduct of trial
3. NYCLA Committee on Professional Ethics; Opinion 754 – Advising a client regarding posts on social media sites
4. New York State Bar Association Committee on Professional Ethics; Opinion 843 - Lawyer's access to public pages of another party's social networking site for the purpose of gathering information for client in pending litigation.
5. New York State Bar Association Committee on Professional Ethics; Opinion 1019 - Confidentiality; Remote Access to Firm's Electronic Files
6. New York State Bar Association Committee on Professional Ethics; Opinion 1019 Confidentiality; use of cloud storage for purposes of a transaction
7. New York City Bar Association Committee on Professional Ethics; Opinion 2010-2 – Obtaining evidence from social networking websites

Selected Sections of the New York State Rules of Professional Conduct

I. Confidential Communication
   - 1.6

II. Presenting, Investigation, or Suppressing Technological Evidence
   - 3.3

- 3.4
- 3.5
- 3.6

III. Technological Communication

- 4.2
- 4.3
- 4.4

IV. Responsibility for Nonlawyers

- 5.3

CYBER ISSUES AND DOMESTIC VIOLENCE: ARTICLES, STATUTES AND CASE LAW

Janet R. Fink, Deputy Counsel
New York State Unified Court System
July, 2012

Articles and Treatises

■ Social Networking and Techological Abuse – Constitutional, Ethical and General Issues

Joshua Azriel, *Social Networking as a Communications Weapon to Harm Victims: Facebook, MySpace and Twitter Demonstrate a Need to Amend Section 230 of the Communications Decency Act*, 28 John Marshall J. of Computer and Information Law 415 (Spring 2009)

Laurie L. Baughman, *Friend Request or Foe? Confirming the Misuse of Internet and Social Networking Sites by Domestic Violence Perpetrators*, 19 WIDENER L.J. 933, 954 (2010)

Mark A. Berman, *State E-discovery: The Ethics of Social Networking Discovery*, N.Y.L.J., Nov. 2, 2010

Katherine Fisher Clevenger, *Spousal Abuse Through Spyware: The Inadequacy of Legal Protection in the Modern Age*, 21 J. Am. Acad. Matrim. Law 653 (2008)

Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 Colum. J. Gender & L. 224 (2011)

Cynthia Fraser, Erica Olsen, Kaufeng Lee, Cindy Southworth & Erica Tucker, *The New Age of Stalking: Technological Implications for Stalking*, 61 Juv. & Fam. Ct. Journal #4:39 (Nov. 2010)[www.nnedv.org]

Hector Gonzalez, James McGuire & Rebecca S. Kahan, *Do Privacy Rights in Electronic Communications Exist?: Courts are proceeding cautiously*, N.Y.L.J., Jan. 17, 2012

Devika Kewaltramani, *You Can Tweet But You Can't Hide: Social Networking for Lawyers* , N.Y.L.J., June 30, 2010

Peter Joy & Kevin C. McMunigal, *The Ethical Risks of Technology*, 27 Criminal Justice #2: 57 (American Bar Association, Summer, 2012)

Michael E. Lackey Jr., *Lawyers and Social Media: the Legal Ethics of Tweeting, Facebooking and Blogging* 28 Touro L. Rev. 149 (2012)

Connie Davis Powell, *"You Already Have Zero Privacy. Get Over It!" Would Warren and Brandeis Argue for Privacy for Social Networking?*, 31 Pace L. Rev. 146 (Winter 2011)

Stephen Prignano, *Social Networking: So Much Data, So Little Guidance, So Much Potential Exposure*, N.Y.L.J., Nov. 15, 2010

Rodolfo Ramirez, *Online Impersonation: A New Forum for Crime on the Internet*, 27 Criminal Justice #2: 6 (American Bar Association, Summer, 2012)

Richard Raysman & Peter Brown, *Social Media Data: Discoverability and Ethics*, N.Y.L.J., Dec. 14, 2010

Jeffrey Rosen, *The Deciders: the Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 Fordham L. Rev. 1525 (March, 2012)

Junichi P. Semitsu *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 Pace L. Rev. 291 (Winter 2011)

Mark S. Sidoti, Phillip J. Duffy & Paul E. Asfendis, *Courts Struggle With Social Networking Access Questions Under 1986 Stored Communications Act*, N.Y.L.J., Oct. 4, 2010

Cindy Southworth, Shawndell Dawson, Cynthia Frasser & Sarah Tucker, *A High-tech Twist on Abuse: Technology, Intimate Partner Stalking and Advocacy* (National Network to End Domestic Violence, June, 2005) [http://www.mincava.umn.edu/documents/commissioned/stalkingandtech/stalkingandtech.html]

Stalking Resource Center, *The Use of Technology to Stalk: DVD and Discussion Guide* (Office for Victims of Crime, U.S. Dept. of Jusitce, 2011)

Ken Strutin, *Social Media and the Vanishing Points of Ethical and Constitutional Boundaries*, 31 Pace Law Rev. 228 (Winter 2011)

- **Cyber-bullying, Sexting, Texting and Teen Dating Violence**

Karla Baumler, *Sexting: Is It Teenagers Being Teenagers? Or is it Child Porn?*, 30 Children's Legal Rights Journal #4:43 (Winter 2010)

Alaina Bergerstock *Albany County's Cyber-bullying Law: Is it Constitutional?*, 4 Alb. Gov't L. Rev. 852 (2011)

Break the Cycle Issue Brief #4, *Technology and Teen Dating Violence* (Teen Dating Violence Technical Assistance Center, Dec., 2008)

Susan W. Brenner & Megan Rehberg, *"Kiddie Crime"? The Utility of Criminal Law in Controlling Cyberbullying*, 8 First Amend. L. Rev. 1 (Fall 2009)

Todd A. DeMitchell & Martha Parker-Magagna, *Student Victims or Student Criminals? The Bookends of Sexting in a Cyber World*, 10 Cardozo Pub. L. Pol'y & Ethics J. 1 (Fall 2011)

Joan M. Gilbride & Brian M. Sher, *E-Mail, Text, Facebook . . . Lawsuit? Legal Minefield of Cyberbullying*, N.Y.L.J., Oct.24, 2011

Samantha M. Levin, Note *School Districts as Weathermen: the School's Ability to Reasonably Forecast Substantial Disruption to the School Environment from Students' Online Speech*, 38 Fordham Urb. L.J. 859 (March, 2011)

Caitlin May, *"Internet-savvy Students" and Bewildered Educators: Student Internet Speech Is Creating New Legal Issues for the Educational Community*, 58 Cath. U. L. Rev. 1105 (Summer 2009)

Jennifer McDonald, *Sexting and Excessive Texting: Symptoms of Teen Dating Violence?*, 30 Children's Legal Rights Journal #4:19 (Winter 2010)

New York State Senate Independent Democratic Caucus, *New York's Definitive Cyberbullying Census* June 2012

Bryn Ostrager, *SMS. OMG! LOL! TTYL: Translating the Law to Accommodate Today's Teens and the Evolution from Texting to Sexting,* 48 Fam. Ct. Rev. 712 (October, 2010)

Emily Shaaya, *States Address the Disconnect: Teens in a Sex-crazed Culture,* 27 Criminal Justice #2:18 (American Bar Association, Summer, 2012)

Kelly Tallon, *Addressing Sexting in the Schools*, 30 Children's Legal Rights Journal #4:1 (Winter 2010)

Michael J. Telfer, *Taking the Fight Against Cyber-bullies Outside the School House Gates,* 4 Alb. Gov't L. Rev. 843 (2011)

Thomas Wheeler, *FaceBook Fatalities: Students, Social Networking and the First Amendment,* 31 Pace L. Rev. 182 (Winter 2011)

Jamie Wolf, *Note: the Playground Bully Has Gone Digital: the Dangers of Cyberbullying, the First Amendment Implications, and the Necessary Responses,* 10 Cardozo Pub. L. Pol'y & Ethics J. 575 (Summer 2012)

- **Evidence, Discovery and Proof**

Mark A. Berman, *Who Can Get Your Tweets, and Can You Object?*, N.Y.L.J., July 3, 2012

Patrick M. Connors, *Disclosure of Information on Social Networking Websites,* N.Y.L.J., Sept. 20, 2011

A.K. Dart, *Deleted Files Can Be Recovered* , http://akdart.com/priv9.html (Updated July 17, 2012)

Gaetano Ferro, Marcus Lawson & Sarah Murray, *Electronically Stored Information: What Matrimonial Lawyers and Computer Forensics Need to Know,* 23 J. Am. Acad. Matrim. Law 1 (2010)

Stephen Gassman, *Matrimonial Law in the Digital Age; What You Need to Know about Electronic Evidence and Why,* New York City Bar Association Center for CLE (Nov. 8, 2010)

William Hamilton & Wendy K. Akbar, *E-discovery in the Age of Facebook, Twitter, & the Digital Family: The Ethical Demands for Attorney Competence,* 33 Family Advocate 16 (Fall, 2010)

Gregory P. Joseph, *Internet, Email and Social Media Evidence*, ST051 American Law Institute-American Bar Association Continuing Professional Education 51 (June, 2012)

Monique C.M. Leahy, *Proof of Instant Message, Blog, or Chat as Evidence*. 100 Am. Jur. Proof of Facts 3d 89 (2008; updated 2012)

Shari Claire Lewis, *Courts Grapple with Discovery of Posts*, N.Y.L.J., Feb. 15, 2011

Deborah Jones Merritt, *Social Media, the Sixth Amendment, and Restyling: Recent Developments in the Federal Law of Evidence*, 28 Touro L. Rev. 27 (2012)

Marjorie A. Shields, *Discovery of Deleted E-mail and Other Deleted Electronic Records,* 27 A.L.R.6th 565 (2007, updated 2012)

Zitter, *Annotation, Authentication of Electronically Stored Evidence, Including Text Messages and E-mail*, 34 ALR 6th 253 [2008]

Statutes

Electronic Communications Privacy Act, 18 U.S.C. §2501 *et seq.*

Stored Communications Act, 18 U.S.C. §2701 *et seq.*

Ethics Opinions

NYC Bar Assoc. Formal Opinion 2012-2: *Jury Research and Social Media* (2012)

NYC Bar Assoc. Formal Opinion 2010-2: *Obtaining Evidence From Social Networking Websites* (2010)

NY County Lawyers Assoc. Comm. On Professional Ethics Formal Opinion #743: *Lawyer Investigation of Juror Internet and Social Networking Postings During Conduct of Trial* (May 18, 201)

NYS Bar Association Comm. on Professional Ethics Opinion 843: *Lawyer's Access to Public Pages of Another Party's Social Networking Site for the Purpose of Gathering Information for Client in Pending Litigation* (9/10/2010)

Case Law[1]

- **Electronic Communication, Social Networking and No-contact Orders of Protection**

A. **New York State Cases**

Matter of Jennifer G. v Benjamin H., 84 A.D.3d 1433, 923 N.Y.S.2d 249 (3rd Dept., 2011)(affirmed modification of custody order to give mother exclusive legal custody, although father's parenting time should not have been reduced; father, *inter alia*, committed the family offense of aggravated harassment by sending an e-mail to mother's sister disparaging the mother that was intended to reach mother)

Matter of Julie G. v. Yu–Jen G., 81 A.D.3d 1079, 917 N.Y.S.2d 355 (3rd Dept., 2011)(Family Court family offense of aggravated harassment 2° affirmed where father sent 294 e-mails to mother that made her ill, despite her repeated requests to limit his e-mails to issues regarding the visitation; affirmed five-year order of protection since father's contact with State Police constituted willful violation of order of

[1] Jessica Ruoff assisted in the preparation of the case law summary.

protection supporting finding of aggravated circumstances)

Matter of Ashley D., 55 A.D.3d 605, 866 N.Y.S.2d 222 (2d Dept.,2008)(affirmed juvenile delinquency adjudication for assault and order placing juvenile on probation with prohibition against using computer except for educational purposes; juvenile had bragged about her crime on MySpace with a link to a YouTube video of the crime in violation of earlier Family Court order)

Matter of Shannon M. v. Michael C., -Misc.3d-, 2012 WL 2877566 (Fam.Ct., Kings Co., July 10, 2012), N.Y.L.J., July 19, 2012 (court dismissed family offense proceeding where, after connecting through the social networking service "J-Date," the parties exchanged numerous chat messages; the messages reflected "ordinary fraternization," first on a social and then on a business level, but did not establish an intimate relationship so as to provide Family Court jurisdiction under Family Court Act §812(1))

People v. Fernino, 19 Misc.3d 290, 851 N.Y.S.2d 339 (Crim. Ct., Rich. Co., 2008)(denied motion to dismiss criminal contempt 2° information since sending a "Friend Request" from MySpace may violate no-contact temporary order of protection issued by Family Court in a juvenile delinquency case)

People v. Welte, 920 N.Y.S.2d 627 (Webster Town Ct. Monroe Co. 2011)(dismiss criminal contempt 2° and stalking 4° charges as insufficient; defendant's accessing complainant's list of "friends" on her Facebook account and sending them letters accusing complainant of using their children against him did not violate order of protection that prohibited contact with her either directly or through a third party; dismissed criminal contempt since order of protection did not prohibit contact with her Facebook "friends;" dismissed stalking since pleading insufficient to establish the four elements – lack of legitimate purpose, course of conduct, material harm and prior demand to cease.)

B. <u>Cases in Other Jurisdictions</u>

U.S. v. Jeffries, 2010 WL 4923335, report and recommendation adopted, 2010 WL 4923324 (E.D.Tenn. Oct 22, 2010) (NO. 3:10-CR-100)[not reported in F.Supp.](adopted magistrate's recommendation to deny defendant's motion to dismiss indictment for knowingly transmitting a threat of physical harm in interstate commerce where a video was posted on YouTube and Facebook threatening to kill and injure a local judge, as well as his ex-wife for alienating his child from him; threats ere not protected speech)

Byron v. Byron, (Ct. Common Pleas, Hamilton Co., Ohio, Jan. 25, 2012) [available on-line at http://westlawinsider.com/wp-content/uploads/2012/03/Facebook-Harassment-Order.pdf] (husband's abusive, disparaging Facebook posts regarding wife violated order prohibiting direct or indirect contact, husband directed to purge the contempt by posting an apology on Facebook every day for 30 days)

C.L.C. v. Bowman, 249 Or.App. 590, 277 P.3d 634, 2012 WL 1526260 (Or. Ct. App. May 2, 2012)(reversed termination of respondent's Stalking Protective Order on the ground that court improperly ruled that it could not consider respondent's blog postings on social networking web-site, where both parties were members, including a comment on petitioner's boyfriend's profile; although not direct threats, the postings could be considered in the context of other contacts between the parties)

Barber v. Keas, 2011 WL 5009850 (Tex. App. Oct. 20, 2011)(affirmed granting of order of protection on ground of likelihood of further violence against former dating partner, in part because defendant posted a "veiled threat" on Facebook, *i.e.,* ""[t]hat he would never-never intentionally put a person in a position to

fail, but being put in that position, that he'll still be standing when the dust clears" in addition to other comments on his Facebook page that made his former dating partner feel unsafe)

Ohio v. Yambrisak, 2011 WL 4974850 (Ohio Ct. App. Oct. 17, 2011)(reversed contempt of court for violation of mediation "no contact" agreement where trial court permitted prosecution to call defendant as a witness against himself in violation of his Fifth Amendment rights; defendant had been charged with posting blogs referencing the complainant)

Andrews v. Ivie, 956 N.E.2d 720 (Ct. App. Ind., 2011)(civil protective order affirmed, since stalking course of conduct during 1 ½ -year period was demonstrated by 64 pages of e-mails, as well as texts, Facebook messages and gifts that were alarming to former girlfriend)

Johnson v. Arlotta, 2011 WL 6141651 (Minn. Ct. App. Dec. 12, 2011)(affirmed extension of Harassment Restraining Order, although reduced duration from 51 to statutory maximum of 50 years; although not communicating directly with complainant, defendant had violated the "no-contact" order by creating a blog entitled "Help Ann Johnson," the complainant, which discussed his relationship and personal information about the complainant in the third person, not identifying himself as author; defendant publicized and promoted the blog by sending electronic messages to the complaiant's relatives and friends, posting links to the blog on other websites and using fake Facebook identities to post the blog to other Facebook users, including the complainant's family)

Dockery v. Dockery, 2009 WL 3486662 (Tenn. Ct. App. Oct. 29, 2009)(husband's contact with friend of wife through MySpace, asking her to contact wife to ask her to call him, violated "no contact" order of protection; printouts of MySpace communication from the friend's computer properly were authenticated)

People v. Corleone, 2009 WL 1077189 (Cal. Ct. App., 4th Dist., Apr. 22, 2009)(Unpub.)(affirmed conviction for violating temporary restraining order where defendant posted a Craigslist ad pretending to be complainant, posted multiple threats against complainant on his Myspace page, sent her threatening e-mails and one directing her to his Myspace page and posted a threatening blog entry)

Beaston v. Ebersole, 2009 Pa. Super 243, 986 A.2d 876 (Pa. Super. Ct. 2009)(reversed order returning computers to defendant because there was a sufficient nexus between his computers and his criminal contempt conviction for violation of a "protection from abuse" order; he sent a disturbing e-mail to ex-dating partner [complainant]'s sister, using an e-mail address which included complainant's initials, job occupation and the word "killer;" he created a MySpace page, which identified him as the "Skankn8er"["Skank" refers to complainant and the "n8er" is a form of "terminator", making him the "Skankinator"]; his MySpace page played a song "I Used to Love Her But I Had to Kill Her," contained the headline "Justice is Coming" and included a posting in which he threatened her; after he "friended" some of complainant's friends, they alerted her ro the postings)

Bedinghaus v. Adams, 2009 WL 279388 (Tex. App., Ft. Worth, Feb. 5, 2009)(affirmed granting of protective order against former dating partner, ruling that the complainant has a reasonable basis for fear as a result of the following pattern of conduct: defendant sent 600 to 800 text messages and e-mails to complainant, some of which were threatening; he sent an invoice to complainant indicating that he hired a private investigator to follow her, printed derogatory statements about her and sent them to her friends, family, neighbors, and employer; he created blogs on which he posted statements referring to her; he came onto her property and he told her that he saw her while she was vacationing out of state)

Rios v. Fergusan, 51 Conn.Supp. 212, 978 A.2d 592 (Superior Ct., CT., 2008)(posting of threatening video by respondent in North Carolina on YouTube was properly prosecuted as tortious act in Connecticut under its long-arm jurisdiction. citing "New York's similar long arm statute," and justified issuance of civil restraining order; assertion of personal jurisdiction over respondent did not offend due process as satisfied criteria of minimum contacts and reasonableness; posting video was not simply passive act on public site but was targeted specifically against petitioner by threatening physical harm)

Odden v. Rath, 730 N.W.2d 590 (N.D. 2007)(affirmed extension of "no-contact" order of protection against father where he had sent mother an e-mail and posted messages on the message-board on his web-site discussing the mother and the custody dispute in violation of the order)

- **Harassment and Bullying**

A. New York State and Federal Cases

T.K. v. NYC Dept. Of Education, 779 F.Supp.2d 289 (E.D.N.Y. 2011)(denied dismissal of parents' claim child was deprived of Free Appropriate Public Education under federal *Individuals With Disabilities Education Act* since school personnel were "deliberately indifferent" to, or failed to take reasonable steps to prevent, bullying, but granted dept.'s motion regarding the child's Individualized Education Plan; student's right to privacy and to be let alone includes right to security + there is no "constitutional right to be a bully")

Finkel v. Dauber, 29 Misc.3d 325, 906 N.Y.S.2d 697 (Sup.Ct., Nassau Co., Jul 22, 2010)(disparaging messages about plaintiff regarding sex and HIV, as well as doctored photos, on Facebook group did not constitute defamation, nor could parents of teen-age group members be liable for tort of negligent entrustment of computer to the teens as a dangerous instrument causing harm)

People v. Rodriguez, 19 Misc.3d 830, 860 N.Y.S.2d 859 (Crim. Ct., Kings Co., 2008)(granted motion to dismiss complaint charging aggravated harassment 2°, harassment and endangering welfare of a child where defendant allegedly sent messages, including "we need to be together," "I will never stop talking to you," and "I love you," to 14-year old on MySpace social networking site; complainant recognized photo and MySpace name but messages were protected speech, not threats, and suggestion to her that she disobey her father in order to join him were insufficient to constitute endangerment)

People v. Kochanowski, 186 Misc.2d 441, 719 N.Y.S.2d 461 (App. Term, 2d Dept., 2000), *lve. app. denied*, 95 N.Y.2d 965 (2000) (affirmed aggravated harassment 2°conviction where defendant set up anonymous web-site with suggestive photos of ex-girlfriend, along with her name, telephone number and address, after break-up, and solicited third parties to contact her, although he did not do so directly himself; criminal contempt conviction reversed because order of protection contained no directives to take down the web-site, since ex-girlfriend was not yet aware of it, and order of protection was not served until after the web-site had been created)

People v. Munn, 179 Misc.2d 903, 688 N.Y.S.2d 384 (Crim.Ct., Queens Co., 1999)(denied motion to dismiss aggravated harassment 2° charge for posting threat to police officer on an Internet "newsgroup;" posting was an electronic communication and inclusion of police officer's name "transformed the communication to one not only intended for the general public, but specially generated to be communicated to" the officer)

B. Cases in Other Jurisdictions

D.C. v. R.R., 182 Cal.App.4th 1190, 106 Cal.Rptr.3d 399, 254 Ed. Law Rep. 305 (Ct. App., 2nd Dist., Calif., 2010) (affirmed denial of defendants' motion to strike plaintiffs' suit under "strategic lawsuit against public participation" (SLAPP) statute; plaintiff, a 15-year old high school student, and his parents sued other students and parents for hate crime, defamation and intentional infliction of emotional distress as a result of a student posting a desire on plaintiff's web-site to "rip [his] heart out" and pound [his] head with an ice pick;" defendants failed to demonstrate that the posting was protected speech)

A.B. v. State of Indiana, 885 N.E.2d 1223, 231 Ed. Law Rep. 921 (Sup. Ct., Ind., 2008)(reversed juvenile delinquency adjudication as evidence of "vulgar tirade" against school principal on student's private MySpace profile page did not constitute harassment, *i .e.*, communication intended to harass, annoy or alarm; student's privacy settings made it unlikely principal would see the posting)

■ Evidence, Discovery and Proof

A. New York State Cases

People v. Agudelo, 96 A.D.3d 611 (1st Dept., 2012)(affirmed grand larceny 3° conviction where complainant adequately authenticated a print-out of the cell-phone instant messages on complainant's cell-phone that had been exchanged with defendant; complainant testified defendant's name appeared on her phone when she received them and a detective testified he had seen the messages on the complainant's phone and the print-out of the messages; court distinguished *People v. Clevenstine, infra*, where MySpace provided testimony, since in *Clevenstine,* that testimony was essential to establish sender's identity)

Patterson v. Turner, 88 A.D.3d 617, 618 (2d Dept. 2011) (plaintiff's online Facebook postings were not shielded from discovery merely because plaintiff used the service's privacy settings to restrict access).

People v. Clevenstine, 68 A.D.3d 1448, 891 N.Y.S.2d 511 (3rd Dept., 2009)(affirmed rape 3° conviction, *inter alia,* because the computer disk containing instant MySpace messages between defendant and two victims was sufficiently authenticated; "both victims testified that they had engaged in instant messaging about sexual activities with defendant," a State Police investigator testified that he retrieved the messages from the computer used by the victims, a legal compliance officer for MySpace testified that the messages on the disk had been exchanged by users of accounts created by defendant and the victims, and defendant's wife testified that she had seen the sexually explicit conversations on defendant's MySpace account)

People v. Givans, 45 A.D.3d 1460, 845 N.Y.S.2d 665 (4th Dept., 2007)(convictions for criminal possession of controlled substance, conspiracy and unlicensed operation of a vehicle affirmed as modified; court held, *inter alia*, that it was error to admit cell-phone text message sent to defendant without evidence he ever retrieved or read it and without authentication of its accuracy or reliability and, further, that it was error to permit jury to access entire contents of the cell-phone, including items not admitted into evidence)

People v. Pierre, 41 A.D.3d 289, 838 N.Y.S.2d 546 (1st Dept., 2007)(affirmed murder 2°conviction, *inter alia*, because Internet instant message sent by defendant to victim's cousin and threatening voice-mail from defendant on victim's phone were properly authenticated; although victim's cousin didn't print or save the instant message and no technical evidence was offered by the Internet service provider or others as to its authenticity, an accomplice witness, a close friend of defendant, testified to defendant's screen

name and the cousin testified that she sent an instant message to that screen name and received a reply; also, the content of the instant message made no sense unless it was sent by defendant and there was no evidence that anyone had a motive, or opportunity, to impersonate defendant by using his screen name; the voice-mail was authenticated by a witness who recognized defendant's voice)

Smith v. Smith, 24 A.D.3d 822, 804 N.Y.S.2d 854 (3rd Dept., 2005)(reversed grant of order of protection to wife in family offense proceeding alleging aggravated harassment 2° where she failed to prove that her husband had been the sender of three threatening e-mails to three e-mail addresses that she established after they separated; the first message appeared to come from wife's former Yahoo ! account, the second from a previously unidentified address and the third appeared to be a message from a person with the wife's name that had been forwarded to her sister; the Court held that "Even assuming that respondent could access her former Yahoo account to send the first message, this record contains no evidence that links respondent to the other two messages or which establishes that he knew the addresses to which these e-mail messages were sent." 804 N.Y.S.2d at 855-856.)

People v. Foley, 257 A.D.2d 243, 692 N.Y.S.2d 248 (4th Dept., 1999)(affirmed conviction for promoting sexual performance by a child and attempted dissemination of indecent material to minors, since computer disk containing conversations between undercover trooper and defendant, as well as graphic images sent by defendant to trooper, were properly admitted; contents were unique and were authenticated by trooper; court also ruled indecent dissemination law not vague or overbroad and not protected speech)

People v. Harris, -Misc.3d-, 2012 WL 2533640, 2012 N.Y. Slip Op. 22175 (N.Y. Crim. Ct. N.Y. Co., June 30, 2012), N.Y.L.J., July 5, 2012 (denied Twitter's motion to quash prosecutor's subpoena, rejected 4th Amendment, federal *Stored Communications Act* and NYS legal arguments, after earlier denial of defendant's motion; Twitter directed to produce arrested Wall St. Occupier's user account information and "tweets" between Sept. 15th and Dec. 30, 2011 in disorderly conduct charge stemming from Brooklyn Bridge demonstration; access to "tweets" after Dec. 30th require a warrant; as the recipient of the prosecutor's subpoena, Twitter, but not defendant, had standing to challenge it; Twitter users have no proprietary interest or reasonable expectation of privacy in publicly posted "tweets," especially since Twitter signed agreement with Library of Congress to archive all "tweets" and states in its Terms of Service that it is "primarily designed to help you [the user] share information with the world"; court noted that the change to Twitter's Terms of Service, effective May 17, 2012, made only <u>after</u> the denial of defendant's motion to quash, now provide that "You Retain Your Right to Any Content You Submit, Post or Display on or Through the Service;" court also rejected Twitter's argument that compliance with the subpoena would be a burden) [<u>note</u>: Twitter has indicated it will appeal. *See* T. El-Ghobashy, "Twitter to Appeal Occupy Decision," *Wall St. Journal*, July 20, 2012]

Matter of B.M. v. D.M., 31 Misc.3d 1211(A), 927 N.Y.S.2d 814 (Table), 2011 WL 1420917 (N.Y.Sup.), 2011 N.Y. Slip Op. 50570(Unreported disposition) (in divorce action, wife's testimony acknowledging authorship and accuracy of blog- posts regarding belly-dancing on websites tribe.net, facebook.com, and myspace.com was used to refute her allegations that an injury caused permanent disability preventing physical activity)

People v. Lenihan, 30 Misc.3d 289, 911 N.Y.S.2d 588 (Sup.Ct., Queens Co.,.2010)(court declined to permit defendant to cross-examine two prosecution witnesses regarding photos his mother printed from MySpace that allegedly depicted the witnesses and victim making hand gestures and wearing clothing that suggested an affiliation with the "Crips" gang; court held "[i]n light of the ability to 'photo shop,' edit

photographs on the computer," the photos could not be authenticated)

Schreiber v. Schreiber, 29 Misc.3d 171, 904 N.Y.S.2d 886 (Sup. Ct., Kings Co., 2010)(in matrimonial action, court denied wife's application for entire hard drive of husband's office computer containing financial data to be deposited with clerk of court for forensic examination or for wife's expert to copy it)

Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657 (Sup. Ct., Suffolk Co. 2010) (court granted the defendant's motion to access plaintiff's current and historical Facebook and Myspace pages and accounts, including deleted pages; court directed plaintiff to sign an authorization and consent and reasoned that plaintiff did not have a reasonable expectation of privacy in light of the policies of both social network companies)

Gurevich v. Gurevich, 24 Misc.3d 808, 886 N.Y.S.2d 558 (Sup.Ct., Kings Co., 2009)(in matrimonial action, wife was permitted to introduce e-mails she obtained from husband's e-mail account after they separated using the password he had given to her while they were together, notwithstanding Penal Law §250.05, the eavesdropping statute, since the e-mails were already stored in his account, not intercepted while in transit)

Matter of D.M. v. J.E.M., 23 Misc.3d 584, 873 N.Y.S.2d 447 (Fam. Ct., Orange Co., 2009)(in family offense proceeding alleging that father sent vulgar messages to mother containing false allegations of sexual abuse of child, court approved subpoena directing Yahoo !, the Internet Service Provider, to disclose only information identifying father as holder of the e-mail account and the contents of e-mail messages sent from that account to the mother's e-mail account during a designated time-frame)

Matter of Bill S. v. Marilyn S., 8 Misc.3d 1013(A), 801 N.Y.S.2d 776 (Table), 2005 WL 1645339, 2005 N.Y. Slip Op. 51093(Sup.Ct., Nassau Co., 2005) (Unreported Disposition)(subpoena of e-mails, telephone logs and three years of AOL instant messages chat logs to establish divorce grounds rejected as overbroad; court noted that more latitude is afforded to discovery regarding financials, as compared to grounds)

Byrne v. Byrne, 168 Misc.2d 321, 650 N.Y.S.2d 499 (Sup. Ct., Kings Co., 1996)(in matrimonial action, court granted wife's motion for discovery of information stored on a laptop computer used by husband, as well as by the children, in the marital residence although owned by his employer, subject to exclusions on the ground of attorney-client privilege; wife's taking possession of "family" laptop not improper)

B. <u>Cases in Other Jurisdictions</u>

Crispin v. Christian Audigier Inc., 717 F. Supp. 2d 965, 974 (C.D. Cal. 2010) (party has standing to challenge a subpoena to a third party defendant where the party had personal interest in the postings and messages on Facebook and Myspace and had standing to challenge the subpoena, citing federal *Stored Communications Act*, 18 U.S.C. § 2703; case remanded to determine whether the party's privacy settings on Facebook and Myspace granted limited access to the party's page and, based on this finding, whether the motion to quash should be granted, *e.g.*, if the party's privacy settings restricted access to a limited few instead of the general public, the party's motion quash the subpoena could be granted)

People v. Rodriguez, 128 Nev. Adv.Op 14, 273 P.3d 845 (Sup.Ct., Nev., 2012)(failure to authenticate 1o out of 12 text messages was error but harmless; citing *Commonwealth v. Koch, infra,* court held that

evidence is needed to show not simply that messages came from a particular phone, but that the alleged author of the messages was the one who actually sent them since others might have used the phone)

State v. Eleck, 130 Conn.App. 632, 23 A.3d 818 (Conn.App.,2011)(affirmed conviction of assault with dangerous instrument where defendant failed to authenticate print-out purporting to be electronic messages sent from prosecution witness' Facebook account; witness indicated her account had been "hacked;" networking site not high-security and content of messages not so distinctive as to necessarily point to witness as author)

*Commonwealth v. Koch***,** 39 A.3d 996 (Pa.Super.Ct., 2011)(substance conviction reversed because police detective's transcriptions of text messages on defendant's cell-phone were not properly authenticated and error was not harmless; while phone was found on a table near defendant, the prosecution conceded that defendant did not author all of the text messages on her phone; prosecution offered no direct proof in the form of testimony from recipients or other possible authors of the text messages and the contents of the messages did not provide any circumstantial evidence as to authorship; while text messages are unique to the cell-phone from which they were sent, the owner of the cell-phone does not necessarily have exclusive access to it) [Note: pending appeal: *appeal granted*, 44 A.3d 1147 (Pa. May 15, 2012)]

State v. Ruggiero, 163 N.H. 129, 35 A.3d 616 (Sup.Ct., N.H., 2011)(affirmed conviction for falsifying physical evidence and filing a false report, *inter alia*, on the ground that e-mails sent by defendant to her divorce attorney, the assistant attorney general and prosecutor were properly authenticated in testimony by both the assistant attorney general and divorce attorney)

Tienda v. Texas, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012) (affirmed murder conviction, as admission of MySpace profile print-outs was adequately authenticated by circumstantial evidence indicating that it was created and maintained by defendant; the web-page print-outs contained photos of defendant and referred to the victim's death, to music played at his funeral, to defendant's gang and to the electronic monitor that was a condition of his house arrest pending trial; also, the web-page print-outs indicated that defendant was the author and referenced his nick-name and e-mail address)

Vermont v. Simmons, 27 A.3d 1065, 1071 (Vt. 2011)(affirmed denial of defendant's motion to suppress evidence obtained by subpoenaing Myspace, since defendant had no reasonable expectation of privacy; Myspace Terms of Service privacy policy authorized disclosure of account information if necessary to respond to a subpoena)

Griffin v. Maryland, 419 Md. 343, 19 A.3d 415, 427-28 (Md. 2011)(reversed conviction for insufficient authentication of printout of image from defendant's girlfriend's MySpace page ostensibly containing her picture, date of birth and location and identifying the defendant; prosecution failed to inquire whether MySpace account was hers or whether she produced its contents and offered no extrinsic evidence about how the police obtained the printout or how it was linked to the girlfriend; no evidence was presented as to search of owner of computer used for the posting or as to efforts, if any, to obtain the information from MySpace to link the profile and posting to the girlfriend)

Commonwealth v. Purdy, 459 Mass. 442, 945 N.E.2d 372 (Sup. Jud. Ct.,Mass., 2011)(affirmed conviction for maintaining house of prostitution; e-mails allegedly sent by defendant were properly authenticated; they were sent from defendant's e-mail address, were on the hard drive of a computer defendant that he said he owned and were accessible through the passwords he provided from memory to the police; one e-

mail contained a photo of him and another described his unique combination of businesses as a hair stylist, masseur and art/antiques dealer; defendant's argument that others had access to the computer and sent the e-mails and that there was no direct evidence of observation of defendant preparing and sending the e-mails related to weight, not admissibility)

Commonwealth v. Williams, 456 Mass. 857, 869, 926 N.E.2d 1162 (2010) (although it "did not create a substantial likelihood of a miscarriage of justice," testimony regarding a MySpace message should not have been admitted in absence of evidence authenticating authorship, indicating whether alleged author had exclusive access to the account, not simply that it appeared to come from a particular account; evidence was insufficient regarding MySpace security and whether site was password-protected)

Dockery v. Dockery, 2009 WL 3486662 (Tenn. Ct. App. Oct. 29, 2009)(copies of print-outs of MySpace contacts from computer of friend of wife sufficiently authenticated so as to be admissible; husband's contact with friend of wife through MySpace, asking her to contact wife to ask her to call him, violated "no contact" order of protection)

Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 39 (Minn. Ct. App. 2009). The plaintiff subpoenaed the defendant's computer files, which the defendant received two days after the browser history and temporary internet files had been erased from her computer. *Id.* at 41. The evidence was not able to be obtained, and the court did not impose sanctions on the defendant because the deletion of evidence could have been from standard computer maintenance. *Id.* at 42.

Clearing your Internet History:

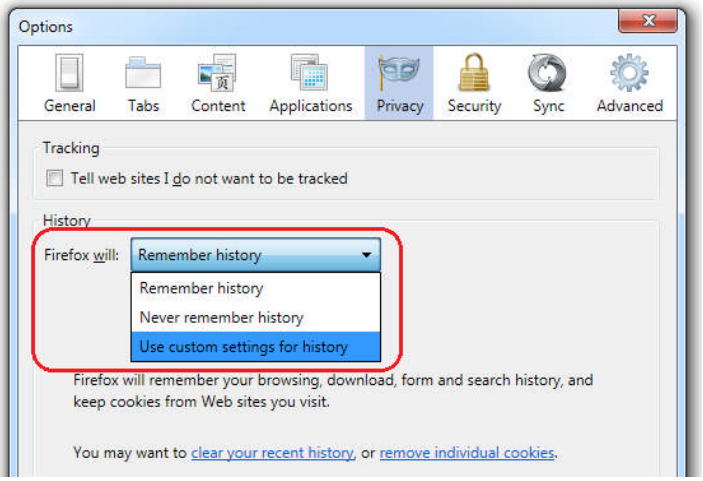
History/Cache file:

If an abusive person knows how to read your computer's history/cache file (automatically saved webpages and graphics), he or she may be able to see information you have viewed on the Internet.

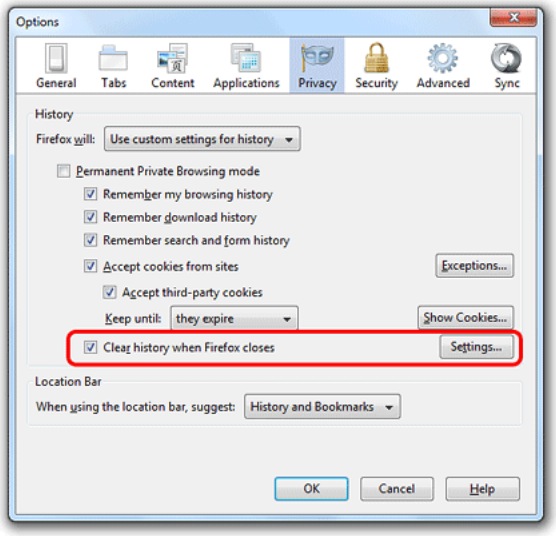
You can clear your history or empty your cache file in your browser's settings.

Mozilla Firefox:

- At the top of the Firefox window, click on the Firefox button and then select Options
- Select the Privacy panel.
- Set **Firefox will:** to **Use custom settings for history**.



- Check the box for **Clear history when Firefox closes**.



- To specify what types of history should be cleared, click the Settings... button next to **Clear history when Firefox closes**.

- In the **Settings for Clearing History** window, check the items that you want to have cleared automatically each time you quit Firefox.

- After selecting the history to be cleared, click OK to close the **Settings for Clearing History** window.
- Click OK to close the Options window

Internet Explorer:

To delete all or some of your browsing history

1. Open Internet Explorer by clicking the **Start** button. In the search box, type **Internet Explorer**, and then, in the list of results, click **Internet Explorer**.

2. Click the **Tools** button, point to **Safety**, and then click **Delete browsing history**. If you don't want to delete the cookies and files associated with websites in your favorites list, select the **Preserve Favorites website data** check box.

3. Select the check box next to each category of information you want to delete.

4. Click **Delete**.

Google Chrome:

1. Click the Chrome menu on the browser toolbar.
2. Select **Tools**.
3. Select **Clear browsing data**.
4. In the dialog that appears, select the "Clear browsing history" checkbox.
5. Use the menu at the top to select the amount of data you want to delete. Select **beginning of time** to clear your entire browsing history.
6. Click **Clear browsing data**.

Adapted from National Coalition Against Domestic Violence, online at: http://www.ncadv.org/protectyourself/lnternetSafety.php and from the Microsoft, Google, and Mozilla websites.

NNEDV

Email & Online Evidence Collection

Domestic violence offenders frequently misuse email and online spaces to stalk, abuse, terrorize, and monitor victims. Abusers may send messages from random email addresses despite a protection order. They may install spyware on the victim's computer, impersonate the victim to cause more harm, or access the content of the victim's accounts without their knowledge or consent.

Because of the continued threats, and/or exertion of control by the abuser, these actions often cause the victim to continue to be afraid for their safety, and the safety of their children. Typically, the abuser believes that his/her actions cannot be traced, but this often is not the case.

The following tips for evidence collection will help ensure that offenders are held accountable.

Email

The header of an email carries important information that can tell where the email was sent from and possibly who sent it. For that, you would need to find the IP address of the sender. Note that this will not work if the sender uses anonymous proxy servers. It will require additional steps if they are using gmail, as Google removes all identifying information from email headers sent via a gmail account and replaces it with an IP address leased to Google. Because of this you will need to serve a subpoena/court order/search warrant to Google to get the originating IP address information.

What is an IP Address?

An IP address is the numerical code that identifies a particular location used to access the Internet. It's basically the equivalent of a street address of a house. Every device, whether it is a computer or portable device, requires an IP address to connect to the Internet. IP addresses consist of four sets of numbers from 0 to 255, with each set being separated by a dot, for example "66.72.98.236" or "216.239.115.148".

There are two types of IP addresses that can be assigned by an Internet Service Providers (ISP). A **static IP address** (which is always the same) or a **dynamic IP address** (which changes every time you log on). Dial-up users are typically assigned dynamic IP address each time they sign on because it reduces the number of IP addresses they must register.

Note: It will not be possible to identify the original IP address from a forwarded email because the email header gets replaced with a new header when it is forwarded. So if you have the victim forward the email in question to you, the email header containing the suspect's information will be removed

Web: nnedv.org/safetynet Email: safetynet [at] nnedv.org Phone: 202-543-5566

and replaced with the victim's information. To be able to identify the original sender, the full header must be expanded in the original email and printed for collection.

Step 1: Finding the Originating IP Address

IP addresses are found within the header of an email, usually between either square brackets or parentheses' {i.e. [123.456.7.8] or (123.456.7.8)}. Every email has a slightly different process for accessing the full header.

- Depending on the version of Yahoo Mail used, some versions have the option for "Full Header" at the bottom right of the message, others have "View Full Header" located under the settings button located in the top menu bar.
- In Gmail, the choice for "Show Original" is under the options for each email, next to Reply (click on arrow to see options).
- In Hotmail, choose "View Message Source" under the options next to Reply in the email (click on arrow to see options).

Headers are read from the bottom to the top. The first "Received from" line you come to in the header contains the IP address and the date and time the message entered the network. (This is just a note to you and should be deleted:Example below references "x-originating IP" but it is not discussed yet. See below addition.)

Example 1 is an example of a short, but complete email header, noting in red the Originating IP address and the Message ID, a unique ID given by the originating SMTP email server that can help identify the sender, even if the "From" was tampered with. Most email headers you will see are typically longer than the example provided and may contain multiple "Received: from" entries. Also, some email headers will have a line titled, "x-originating-IP:" This should be compared to the first "Received: from" entry you come to. They should match. If they do not, this is one indication the email header may have been tampered with.

Example 1

Return-Path: <bo-bwzv75gbruqgjvau79gjgqcd1etmfu@b.e.redbox.com>
Received-SPF: pass (domain of b.e.redbox.com designates 8.7.43.55 as permitted sender)
d2luZyBvbiBhIG1vYmlsZSBkZXZpY2U_IENsaWNrIGhlcmU8L2ZvbnQ.PC9h
→**X-Originating-IP: [8.7.43.55]** - **(Originating Address)**
Authentication-Results: mta1468.mail.mud.yahoo.com from=e.Redbox.com;
domainkeys=pass (ok); from=e.Redbox.com; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO mta935.e.redbox.com) **(8.7.43.55)**
by mta1468.mail.mud.yahoo.com with SMTP; Mon, 09 Jan 2012 23:21:10 -0800
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; d=e.Redbox.com;
s=20111006; t=1326180070; x=1341904870;
bh=vHcWxB+fko8JnzSoHgJq7o0Sb60=; h=From:Reply-To;
b=aq2hXhNIClf/rE/ckB6HCT+mq94XLXa0gooqa1fP8ZDfLlo0RQ1H8WkbwK/
h=Date:Message-ID:List-Unsubscribe:From:To:Subject:MIME-Version:Reply-To:Content-type;
Date: Tue, 10 Jan 2012 07:21:10 -0000
→**Message-ID:** **(This will be a long series of numbers and letters)**

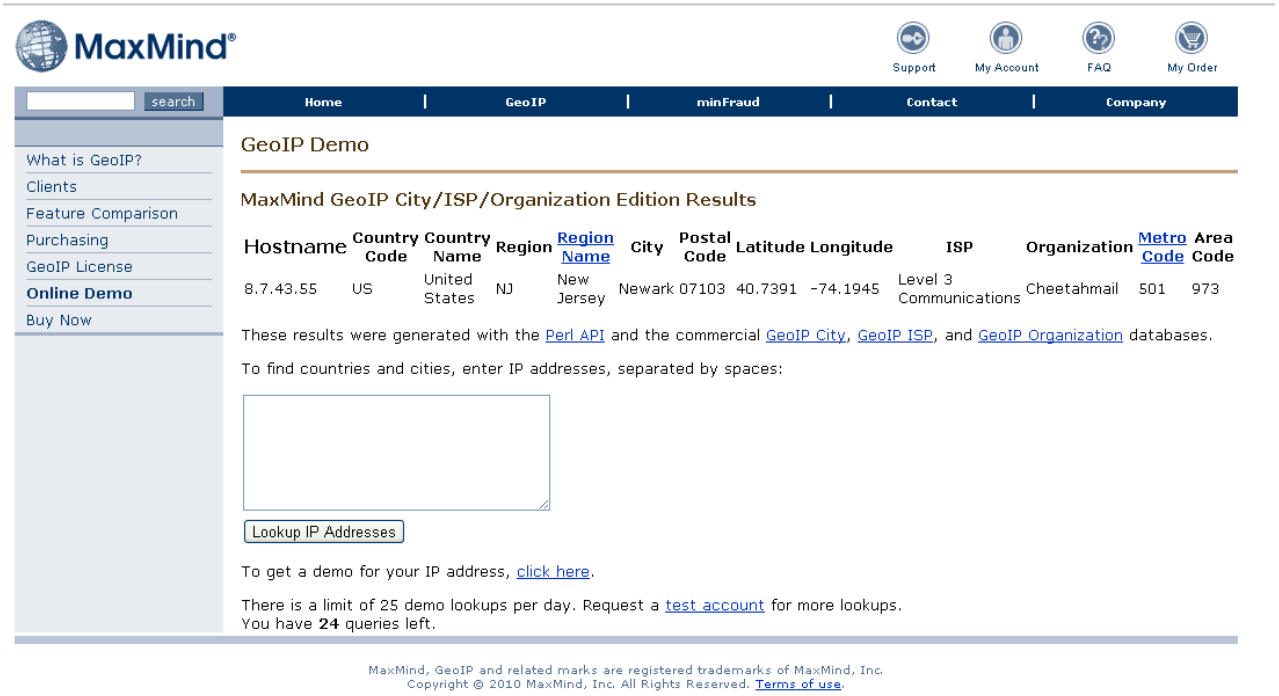
Step 2: Trace the IP Address

Once you have the IP address of the original sender, you can find the Internet Service Provider (ISP). The "WhoIs" search feature on several sites, including www.arin.net & www.geektools.com, will provide the name of the Internet Service Provider, commonly referred to as the ISP, or company that has assigned the IP address to someone (see Example 2).

Example 2

Network	
NetRange	98.231.128.0 - 98.231.255.255
CIDR	98.231.128.0/17
Name	DC-CPE-32
Handle	NET-98-231-128-0-1
Parent	JUMPSTART-5 (NET-98-192-0-0-1)
Net Type	Reassigned
Origin AS	
Customer	Comcast Cable Communications, Inc. (C02058960)
Registration Date	2008-10-06
Last Updated	2008-10-06
Comments	
RESTful Link	http://whois.arin.net/rest/net/NET-98-231-128-0-1
See Also	Upstream network's resource POC records.
See Also	Upstream organization's POC records.
See Also	Related delegations.

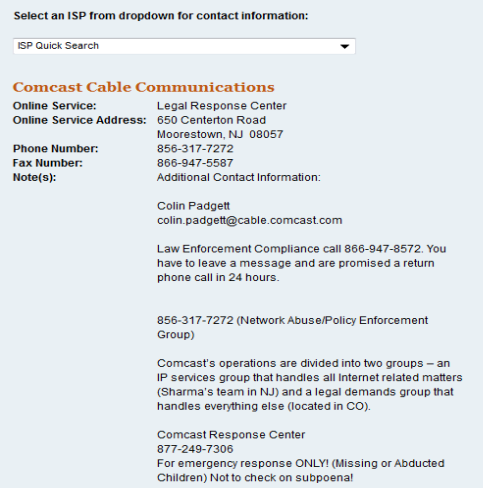
Another useful resource is www.maxmind.com. This site will not only provide you with the ISP information, but will perform a geolocate for the IP address information you are searching for. It is important to recognize the resulting location will only be a general location. Although it may site a particular city, you may find as your investigation progresses it was actually in a neighboring city several mile away. However, this information may still be useful in identifying potential suspects at an early stage of your investigation. Using the IP address from example 1, [8.7.43.55], MaxMind produced the below results:

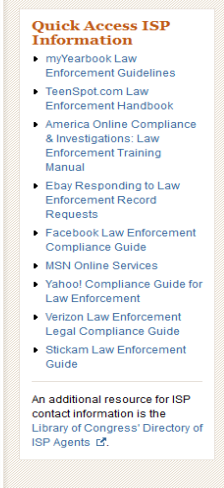


Step 3: Contacting the Internet Service Provider (ISP)

The ISP can identify who the IP address was assigned to. In some cases, it may be an individual home, linking directly to the abuser, or it may be to a hotel, who may then be able to identify who was in that room using that Internet connection. It is important to remember hotel networks can be simple or complex and the amount of information they can provide you may vary dramatically. Even in the worst case scenario, as part of the licensing regulations in most states a law enforcement officer is authorized to view the "guest list" for a hotel at any time (check with your local prosecutors to determine what your individual authority is for your jurisdiction). By doing this you may find your suspect was checked in at the hotel during the date and time the message was sent from the identified IP address.

Most ISP's will have a specific contact for law enforcement. You can search for that specific contact information on the ISP List at www.search.org (found under 'Quick Links', example below). You can also contact the ISP's main number or technical support number if the ISP is not listed or the listed contact information is no longer valid.





With a Retention Notice or Preservation Order, the ISP can lock the account and ensure that nothing will be deleted permanently from their servers or capture what information is associated with a given account at the time of receipt of the preservation order. This is a critical step to ensure information is still available until a subpoena or search warrant can be obtained as a lot of important information is volatile and could be lost forever if not preserved. A subpoena or court order can gather demographic information and a search warrant can provide actual email contents.

Many ISP companies will lock the owner/user(s) out of the account identified in the Preservation Order, and notify the "owner" of the account upon receipt of said order **UNLESS** you specifically request them not to in your preservation order. This is accomplished by simply including a line in your preservation order, and again in the subsequent subpoena, court order or search warrant that states, "Do not lock the user out of the account identified in this document. Additionally, you are specifically request not to disclose or notify the subscriber, "owner" or any users of this [preservation order/subpoena/court order] as it could jeopardize the investigation and create an increased level of risk to the safety of the victim."

Some ISP's may state that they will charge a fee for the processing of the requested information. Informing them that the fee is not feasible often results in it being waived. Additionally, it can also be a cost that is passed on to the offender through restitution fees assigned during the sentencing phase, if the suspect is found, or pleads guilty.

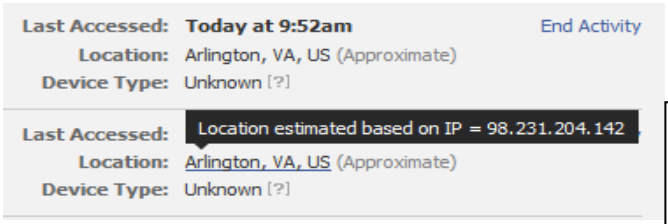
Social Networking & Online Spaces

Victims are increasingly reporting that abusers are harassing them through online spaces, such as Facebook and other social networks. Here are a few of the common concerns and some tips for holding offenders accountable.

Monitoring and Hijacking Accounts

Abusers often access the victim's accounts, either without their knowledge to secretly monitor their computer activity or more blatantly, completely taking over an account to impersonate or embarrass the victim.

Several sites allow users to view past log-in activity, including user location and IP address. Both Gmail and Facebook provide this information.



- Example of Facebook's 'Active Sessions', located under 'Security Settings'.

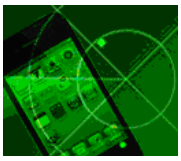
Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your time zone)
Browser	* United States (VA) (98.231.204.142)	1:34 pm (0 minutes ago)
Mobile	United States (VA) (98.231.204.142)	2:21 am (11 hours ago)

- Example of Gmail's 'Account Activity', accessed at bottom of Inbox.

Obtaining an IP address log from the site may provide useful evidence in proving a suspect used this method to harass the victim. This log will provide you with a list of IP addresses and associated dates and times that accessed the account in question. Once you obtain the IP address log, you can look up each IP address that does not belong to the victim. Typically, the victim's IP address will be documented numerous times within the log, but a quick check of the victim's IP address and knowledge of who their ISP is will be very helpful in confirming their IP address. IP addresses identified as unauthorized should be documented and the above listed process of preservation orders, followed up with a subpoena/court order/search warrant, should be followed.

Reprinted with permission The National Network to End Domestic Violence

Cell Phones: Location Tracking & Sharing



How Does the Technology Work?

There are many ways a cell (aka mobile) phone's location can be tracked or shared.

- All U.S. cell phones are required to have some type of location-based technology to enable an emergency dispatch centers to find a 911 caller's real-time location and number. Thus, geographic location tracking capabilities have been integrated into all U.S. cell phones, as well as several international ones.
- Phone carriers tend to use one of two methods to find a mobile phone's location in their network: some cell phones contain **Global Positioning System (GPS)** receivers that connect with GPS satellites to provide the cell phone's location. Cell phones without a GPS device send signals to nearby network cell towers, and use that information to triangulate the cell phone's location.
- Additionally, some cell phones, are designed to be able to connect to the Internet via a **cellular broadband network** and/or via **Wi-Fi network** (aka a local wireless Internet access point). If a cell phone connects via a Wi-Fi network, that connection can also disclose more or less precise information about a cell phone's location depending upon how the Internet Service Provider provides the wireless Internet connection.
- Some cell phones also keep a temporary file of nearby cell phone towers and Wi-Fi hotspots (places that offer local wireless Internet access), to potentially make the cell phone user's connectivity more efficient.

There are many applications and **location-based services (LBS)** available for cell phones that can or might reveal a location, especially if installed or enabled on feature-rich cell phones such as smart phones (e.g,. iPhone, Android, Blackberry). Some cell phones come preloaded with such applications and other phones require someone to install the application onto the cell phone, and create a user name and password in order to begin accessing the location-based service. Some applications may not need a location to function, but may be set to access the cell phone's location anyways (e.g. a dictionary or gaming application). Depending upon the service's or phone's current location privacy settings, a cell phone's location might get shared only with the owner, with multiple cell phones, with the computer the owner sync's the phone to, or even online via a location sharing service's website.

There are different types of location-based services (LBS) available for cell phones, for example:

A. Optional Services Within A Phone Plan. Some wireless carriers offer customers an add-on option to location track any phone that is part of their *family phone plan*. Some providers require that each cell phone in the plan receive and return a text to *allow* the tracking. Other wireless carriers or cell phone makers offer options to remotely locate, lock, or even delete all information on your cell phone, if stolen or lost.

B. Cell Phone Applications. Now a days, people can easily and cheaply install extra cell phone applications that use the phone's current location to obtain directions, nearby places or meetings of interest, weather, or, to even share a location as part of a status update, for example:

- **Navigation, Directions and Mapping.** Some applications use location-based information to provide, log or store real-time directions and maps. Most display a map that tracks the cell phone's turn-by-turn location. Some let you preload maps and directions, others pull in maps as you need them using the cellular broadband network or a Wi-Fi connection, and, others enable you to log or save routes taken and view them later via a phone or website. Some applications are designed to log things like your run, bicycle ride or hike and offer the option for you to share location-based details (route, speed, distance, date, time, name, age, etc.) with others in one or more social networks.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

- **What's Nearby?** Many applications use your cell phone location to tell you what's around you. They let you search for nearby hospitals, grocery stores, restaurants, gas stations, drug stores, coffee shops with free Wi-Fi, deals and discounts, the times movies are playing at local theatres, the times buses or trains leave from nearby stations, current weather, and more.
- **Social Networking & Location Sharing.** Many social networking applications use the phone's current location to find nearby activities or people, and offer to share a location as part of a status update.
  - Some social networking services let people create or join interest-based groups to plan activities and meet up offline and then use the cell phone's location to alert users to nearby and upcoming activities.
  - Some services focus primarily on getting people to do social location sharing (e.g. Foursquare, Loopt, Gowalla). They encourage users to check into nearby spots, post comments or journal entries, upload photos, earn points or badges, receive discounts, or, simply let others know "I'm here now".
  - Even popular social networking services (e.g. Facebook, MySpace, Twitter) that did not initially offer a real-time location sharing, now offer a more specific location options as part of a status update.
  - Many location-based services and applications also make it very easy to share your location across several social networks. For example, a user of one social network can set it to automatically post a status and location update simultaneously to several other social networking sites.
  - Several social location-based services allow the user to make choices about what location is shared. Some offer options such as "exact, city, country" or let individuals choose their own location either from a list of "what's nearby" or by manually entering any location. Some applications, particularly social location sharing applications, allow people by default to share a location for someone else using the same service unless some privacy settings are changed.
- **Cell Phone Cameras & Location Data**. If you use a cell phone camera that has location-tagging enabled, the images might have geolocational data (latitude and longitude) embedded as part of the image file. In most cell phones there is a setting that can turn this feature on or off.

In a majority of cell phones, there are application-level or/and phone-level settings that allow someone to turn location-based features on or off or set portions of a user's social location profile or status updates to public, restricted, or private. Some phones make it easy to find a list of all currently installed applications requesting the cell phone's real-time location and then change their settings; other cell phones make it more difficult for a user to find and change location privacy settings for a particular application or service.

How is it Relevant to Agencies and Partnerships?

- Many staff and volunteers at agencies and partnerships use cell phones with active location-based services and applications. For example, some staff or volunteers map directions between places or take a geo-tagged photograph to document a situation or potential crime. While some cell phones are owned by the agencies, other phones are personally owned. Since some uses of location-based services can place the privacy and confidentiality of victims at risk, it's important for agencies and partnerships to review all use of cell phone-based location services and establish practical policies around staff and volunteer use that promote safety and privacy for all but don't prohibit all use.
- Some agencies and partnerships create social networking pages or presences on sites that people may access via their cell phones and then post updates that include location-based information (e.g. Facebook, Twitter, Flickr). Agencies need to have a policy on how to respond under these circumstances.
- Victims and other visitors to agency buildings bring cell phones with location-based applications and use them while sitting in waiting rooms or visiting other areas of the building or grounds. Some agencies or collocated partnerships can share their location, while others must work hard to keep their agency's location hidden for legal and/or confidentiality reasons. For agencies with confidential locations, such as

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

some domestic violence shelters or transition houses, it is particularly important to inform visitors and residents about privacy settings they might use to prevent accidental location-sharing.

- Some victims and their children may need specific information about privacy risks and safety strategies regarding each location-based application on their cell phone.
- Location-based services on cell phones may be misused to stalk and track victims. Some perpetrators may add optional location tracking services to their family phone plan to secretly track others on the plan. It is not uncommon for perpetrators to misuse social location sharing networks to find places a victim has checked into recently or sometimes even to impersonate a victim on a social location sharing service. Some perpetrators search online for photos of the victim and check to see if it's geo-tagged with a place the victim hung out. In order to hold perpetrators accountable, agencies need to understand what the perpetrator is doing and how to collect timely evidence.
- Cell phone location information can be a vital part of an criminal investigation and used to hold an perpetrator accountable; this may require the court to issue a subpoena or search warrant to the cell phone company provider.

Benefits & Risks

Many victims (their children, family and others they spend time with) use cell phone location-based services.

- Location-based cell phone services can help a victim access needed services and/or support. If a victim is fleeing violence or in the process of relocating, being able to use their cell phone to map directions or look up information can make it easier to navigate a new town or find needed resources and services.
- However, if the victim or her children (or others the victim spends time with) don't know enough about the location privacy or sharing settings of every application or service on their cell phone, they might post status or location updates or photos that accidentally include the victim's location, thus possibly making it easier for the perpetrator to track the victim down.
- There are also safety risks if any of the cell phones used by a victim (or those with her/him) have location tracking enabled as a part of a family phone plan that the perpetrator controls and views. Or, if the perpetrator can access recently used map or direction files on the phone or a computer that the phone's data has been synced with.
- Perpetrators can find the location of buildings many ways; perpetrators can also hide location tracking devices in any belongings or vehicles and a computer's connection to an agency or nearby Wi-Fi network can provide information that discloses some information about location. While some shelters and agencies worry about victims bringing their cell phones with them when they stay at the shelter or come in for services, the solution is not to create rules that prohibit cell phone use, but be prepared to discuss all the risks and benefits with victims and to make new free cell phones available for victims to use if necessary for safety reasons.
- A victim's cell phone may be necessary for her safety. For example, some perpetrators may demand that she must answer her phone, no matter when or where. Not being able to answer her phone may be dangerous to her or those she loves.
- If a victim is in hiding, she may need a cell phone to keep in contact with others via texts, calls or social networking sites. Some victims may have medical issues and need to carry a cell phone in case they need to call for emergency services.

Agencies and partnerships can help victims figure out if the location of their cell phone is somehow being tracked by a perpetrator and then discuss safety strategies and options including changing settings or deleting applications. For example, if the perpetrator is locating a victim through her teenager's social location status updates, the teenager can learn how to increase privacy settings or manually set different locations for future status updates.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

Things to Consider

- How is the victim's location being tracked? Is it via a cell phone, or not? Discuss with the victim the circumstances where a perpetrator seems to know location information. For example, it could be that there is a GPS device hidden in the victim's vehicle or a belonging. Or, it could be that geo-tagged photos of the victim are being posted online by well-meaning acquaintances.
- Is it safe for the victim to turn off the location–based services on the cell phone? Or is it safe for the victim to temporarily remove the battery if she/he is planning secret travel? Is it safe to do so? Discuss risks with victims before they travel to your agency or other secret place.
- Is the victim comfortable contacting the cell phone carrier to ask if a location tracking service is activated on the cell phone or how to disable all location services but 911 calls?
- Some cell phones allow the user to turn "Location On / Off" under Menu Settings or Options such as "GPS Services" or "911 only" or "Privacy > Location" or "Location Services". A few phones even list all applications that want to use the phone's location services and allow the user to turn location services on or off for each individual application, such as the phone's camera.
- If the cell phone's location sharing is hard to disable and the perpetrator can somehow see the cell phone's location, could the victim get another cell phone, and get rid of the tracked phone?
- Is the victim (or any children) using any social networking or location sharing applications on their cell phones? Can these be set to share a more private or different location? Sometimes the cell phone application will clearly describe how to turn on or off location tracking or how to change privacy settings to specify who is allowed to see the location; other times, the victim will need to call the phone provider or search online to learn how that application's location tracking settings might be changed on their specific phone.
- Is there a benefit to simply uninstalling the location-based application from the cell phone? Most phones list applications somewhere (under a menu such as Options or Settings). Most applications can be uninstalled but some preloaded applications cannot. When preloaded applications cannot seem to be removed from the cell phone, the victim can learn about the application's location-based tracking or sharing settings options and decide whether to disable location settings for that application. If it is unclear whether an application is on the phone, where its' setting are, and whether it can be uninstalled, victims can search for an answer online or contact the phone maker (e.g. Apple makes iPhones, Google makes Android) or phone carrier (e.g., AT&T, Verizon Wireless, Sprint) and ask them to walk her through how to find this information in the phone.
- If the victim's location privacy has been compromised, does the victim want or need to relocate? What steps might be taken with respect to cell phones and location based-service to increase the victim and her children's safety during and after relocating?
- Depending upon the location-based application or service used, how will law enforcement best document and collect evidence about the perpetrator's misuse? What charges might be appropriate? (e.g. stalking, electronic surveillance).
- If an agency or partnership is using or considering creating pages or profiles on social networking sites it should consider creating policies or interim practices to address situations where an online visitor shares location-based information on its page. Policies should consider how to best address posts with location information, how to provide information to victims about the ways their location might be shared, and, how to discuss emerging ways that location sharing may impact the safety and privacy of victims, their families and friends, as well as agency staff and volunteers.

See NNEDV's tipsheets on: "Social Networking and Privacy Tips for Domestic and Sexual Violence Programs", "Online Privacy and Safety Tips" and "Finding Laws To Charge Perpetrators Who Misuse Technology".

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

Reprinted with permission The National Network to End Domestic Violence

Privacy & Safety Planning With Survivors

Tips When Relocating

Ask Questions

When the health club, video rental store or other business asks for your Social Security Number, don't be afraid to ask why they need it. If you are signing up for an email address or web service, don't give your home address or phone number – they are almost never required. When signing up for traditional land-line telephone service, ask to be unlisted in the telephone directory, and be careful about to whom you share that phone number with. For example, when a cashier asks for your phone number, consider saying, "No, I'd rather not give it," or giving an alternate phone number like your old work number.

Research Address Confidentiality Programs in Your State

These programs allow you to use an alternate address to receive your mail and register to vote. Since 1991 approximately 20 states have established address confidentiality programs for survivors of sexual violence, domestic violence and stalking. Also, ask about receiving mail, shipments, and non-first class mail (magazine subscriptions) since many programs will process only first-class mail.

Change Passwords & PIN Numbers

When you relocate, be sure that you create new passwords for ALL of your accounts, including email, instant message accounts, online accounts, bank accounts, ATM, voicemail, etc. If you suspect that someone has the password to any of your accounts, change your password on a computer that this person doesn't have access to or call the agency and change your passwords or PIN over the phone. The most secure passwords are at least 8 characters long and use a combination of letters and numbers.

Learn Which Records Are Public

Many court systems and government agencies publish records to the Internet. Your driver's license, voter registration, and other records may be public and may be published to the Internet. In addition, if you've made charitable contributions or volunteered for a political party, your information may also have been published online. Ask agencies how they protect or publish your records and request that court, government, post office, and others seal or restrict access to your files to protect your safety.

Search For Your Name on the Internet

Major search engines such as "Google" or "Yahoo" may have links to your contact information. Search for your name in quotation marks: "Full Name". Check online phone directories; unlisted phone numbers may actually be listed especially if you've given the number to a business. Sometimes it's okay to leave certain information online, especially if it's harmless. If you want something removed, the website may have instructions for you to fill out a form or on how to email them. Oftentimes they may ask for personal information to prove your identity. Try not to share more information than they already have because data brokers make money by selling accurate information.

Privacy & Safety Planning With Survivors

Tips When Relocating

Have All Important Records With You Before Relocating

Gather all important records, especially those of your children and pets. Have copies of school and immunization records to share with professionals in your new community. If you relocate without these records, you may have to share your new address with former schools and physicians in order for the records to be mailed to you. Consider asking that the records be mailed to a friend or family member instead. The more places that have your new address, the greater the risk of the abuser finding it.

Utilities in Your Name

Even if you have a PO Box, you'll need utilities (like electricity and water) at your new home. Consider renting an apartment with utilities included or putting the utilities under a roommate's name. Ask local utility providers about their privacy polices and find out if they publish or sell your information.

Consider a Private Mailbox or PO Box & Don't Give Out Your Real Address

When asked by businesses, doctors, and others for your address, give them have a private mailbox address or a safer address. Try to keep your true residential address out of national databases. The U.S. Postal Service will not sign for packages but many of the private companies (Parcel Plus, UPS store, etc.) will sign for a package for you.

Research Voter Registration Policies

Many voter registration offices not only sell your address and other information, but they also publish it to the Internet. Some states will keep your voter registration confidential at your request. Before you register to vote in a new community, research your privacy options, and talk to an election supervisor if needed. It is important that survivors of abuse be able to vote, and it is equally important that their safety not be jeopardized.

Consider Alternatives To Filling Out a Change of Address Form

Consider not providing a forwarding address to the U.S. Postal Service and individually contact people who mail you, or forwarding your mail to a P.O. Box or private mailbox. The large National Change of Address Database (NCOA) provides your new address to many marketing companies, magazine publishers, student loan companies, and others. The more companies that have your address, the more likely it may end up in a Web-based directory.

GREATER BOSTON LEGAL SERVICES
... and justice for all

NNEDV

This project was supported by Grant No.2007-TA-AX-K030 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of theauthor(s) and do not necessarily reflect the views of the Department of Justice, Office oniolence Against Women.

Web: nnedv.org/safetynet • Email: Relocation [at] nnedv.org • Phone: 202-543-5566

NNEDV

Technology Safety Quick Tips

Device	Description / Risks	Safety Strategies
Spyware / Computer & Phone Monitoring Software	▪ It enables a person to secretly monitor someone else's entire computer activity. ▪ It can be installed remotely by sending an email, photo, or instant message. ▪ It runs hidden on a computer. It is very difficult to detect and almost impossible to remove. Some secretly reinstall if removed. ▪ It can record and send screenshots (pictures of what's on the screen), all keystrokes typed, web sites visited, emails sent, instant messages (IM), accounts accessed, passwords typed, and more.	▪ When you first get a new computer or phone, increase security by enabling firewalls for your computer, network or phone (see settings) and install or run anti-spyware and anti-virus software; set your computer or device to automatically install updates. ▪ Don't open any attachments if you don't know the sender, or you suspect abuse. Instead delete the attachment or have IT staff look at it. ▪ Trust your instincts. If someone knows too much about your computer activity, your computer may be monitored. Use a "safer" computer (one the abuser does not have any access to) for private communications and web browsing. ▪ Consider changing passwords and creating new accounts on another computer. Do not access those accounts or use those passwords on the monitored computer.
Keystroke Logging Hardware	▪ It provides a record of all keystrokes typed on a keyboard. ▪ Someone needs physical access to the computer to install and later retrieve the device with the data log of all your keystrokes. ▪ An abuser may use it to see the passwords you type and then be able to access your email, credit card, or bank accounts, etc..	▪ Has someone fiddled with, fixed, or given you a new part for your computer? ▪ Look for a small piece that connects the keyboard cord to the computer; it can also be part of an external keyboard, or something installed inside a laptop. ▪ Change passwords on accounts from another computer and do not access those accounts from the compromised computer. With some services, you can ask to get an alert (e.g. fraud alert) if your password gets changed or your account gets changed.
GPS Devices (Global Positioning Systems)	▪ They are small, easily hidden, and affordable devices that provide the ability to monitor someone's location. ▪ Many cell phones also have GPS devices. ▪ They might be used to track your location real-time (as you move) and to map your location history. ▪ Depending upon the service or	▪ Trust your instincts. If someone seems to know too much or show up in random places, check for hidden GPS devices or other location tracking services. Consider notifying law enforcement. ▪ A device can be hidden in your belongings or vehicle. Check the trunk, under the hood, inside the bumper and seats. A mechanic or law enforcement can also do a search.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

NNEDV

Technology Safety Quick Tips

Device	Description / Risks	Safety Strategies
	application used to access GPS data, the stalker may be able to secretly monitor your location via websites or sometimes via their phone. Some devices must be physically retrieved for the abuser to review your location data.	▪ Safety plan around/before removal of any location tracking device, as it may alert the abuser.
Cell & Mobile Phones	▪ Phones can be a lifeline for victims. ▪ Phones can be hidden inside vehicles as listening devices by using the "silent mode" and "auto answer" features. ▪ Most phones have GPS chips and location tracking abilities, which can be used to determine someone's location. Some abusers install additional applications on a cell phone to track your application. ▪ Logs showing phone usage may be monitored on the actual phone or over the Internet via the phone company's online billing record. ▪ Joint phone plans with an abuser may give that person access to phone features and calling log information. ▪ If your phone has a Bluetooth device, the stalker might try to connect with your phone using the Bluetooth to access information on your phone or intercept your communications.	▪ For additional privacy and safety, consider getting a separate donated phone from a shelter or purchasing a new phone (e.g. a pay-as-you-go phone). ▪ Mechanics or law enforcement can check the vehicle to determine if a phone has been hidden somewhere. ▪ Contact carrier to add a password or code to account to protect from wrongful access. ▪ You can change the phone's location setting to "E911 only" or "911 only" so that the phone company only access your GPS if you dial 911. ▪ Also check if your phone has any applications installed that separately ask to access and use your real-time location, such as for mapping directions. Settings such as "show all/hidden applications" might unveil some hidden applications. Consider turning off or uninstalling these applications. ▪ Use phone settings to change your default Bluetooth password, set Bluetooth to hidden, and turn Bluetooth off. ▪ Always give location information to 911 in an emergency.
Caller ID & Spoofing	▪ Reverse directories can provide location based on a phone number. ▪ Services like Trapcall, can unblock a blocked number without notice. ▪ Caller ID can be spoofed to falsify the number displayed when you get a call. ▪ If you call a person using an Internet phone, your blocked number may be	▪ Survivors can contact the phone company and ask that their phone number be blocked to protect privacy. Blocking is supposed to prevent your caller ID from displaying. However, even with a blocked number, sometimes your caller ID will still display. Consider using another phone or outgoing phone number. ▪ Regularly test the line by calling other phones to

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

NNEDV

Technology Safety Quick Tips

Device	Description / Risks	Safety Strategies
	displayed.	ensure it is blocked. ▪ Use an Internet phone (i.e., Skype) or a pay-as-you-go phone purchased with cash to make calls if you are worried about your number / location being revealed.
Faxes	▪ Fax headers include sender's fax number, which can be used to determine location thru reverse look-up. ▪ Fax machines often now have hard drives and extensive memory. Consider privacy, confidentiality and privilege issues when deciding what fax machine to use. ▪ Electronic faxes (e-fax) are sent through the Internet as email attachments and, like all email, can be intercepted. ▪ Also because e-faxes get sent via a 3rd party and are temporarily stored on a 3rd party Internet server, there are different confidentiality and security risks.	▪ Cover sheet can request that the header be removed before forwarding. ▪ If it's legal, consider changing the outgoing fax number displayed to a different number on a case by case basis for safety or privacy reasons. ▪ Never send personally identifying or sensitive information in an E-Fax. ▪ Make sure you know who is receiving the fax. Call ahead. Some fax machines require the receiver to type in a password to see the fax.
Cordless Phones	▪ Because cordless phones transmit your conversation wirelessly between the base unit and phones, they can more easily be intercepted by scanners, baby monitors, & other cordless phones. ▪ If you do not unplug the base unit, the phone may continue to broadcast for the duration of a call, even after you switch to a corded phone, allowing for the possibility of continued interception.	▪ Switch to a corded phone before exchanging sensitive information. ▪ Unplug a cordless phone from the power source, even after the corded phone has been turned off or hung up to ensure that the current call's conversation won't still be broadcast and overheard. ▪ Best practice is to limit information discussed or not use cordless phones for confidential communications with victims.
TTY (Teletypewriters)	▪ A communication tool for people who are Deaf or hard-of-hearing that connects to a phone line. ▪ Can be misused to impersonate someone. ▪ All TTYs provide some history of the entire conversation. The history and transcripts of TTY calls might be recorded on paper or electronically. The abuser	▪ Create a code word or phrase to ensure the identity of the person on other end and to avoid impersonation. ▪ Regularly clear TTY history unless a cleared history would increase risk. ▪ Best Practice: Agencies should clear their TTY memory, avoid printing transcripts, and shred all printed transcripts of TTY calls, unless the victim

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

Device	Description / Risks	Safety Strategies
	might monitor this information or misuse it; in some cases, a survivor might be able to introduce a transcript of a threatening TTY conversation as evidence.	explicitly requests that one printed transcript be kept for safety or evidence reasons.
Relay Services	▪ A free service where a third party (operator) facilitates a conversation for a person who is Deaf, hard-of-hearing, or has a speech disability. ▪ Users may access relay services via a video phone, web cam, computer, TTY or other device. They might use a phone line, Internet or cable connection. ▪ Can be used to impersonate someone. ▪ Relay conversations and devices may be monitored.	▪ Establish secret code words or phrases to ensure identity of person. ▪ If possible, use a "safer" TTY, device, or computer to access relay (one an abuser hasn't had access to). ▪ Be aware that relay conversations might be secretly recorded by an abuser using spyware or video recording. ▪ When possible, meet in person to discuss sensitive information. ▪ Best practice: Relay services are not a substitute for providing interpreters. Agencies should always offer an in person certified sign language interpreter. Additionally, agencies can contract with Video Remote Interpreter (VRI) services. These are not video relay services but use similar technologies; an agency would need to have a high speed connection and video phone or web camera. An agency can contract with a VRI provider to be on call remotely 24X7 in case a survivor arrives and needs an interpreter quickly.
Email	▪ It is like a postcard and is not a private form of communication. ▪ Can be monitored and intercepted in a variety of ways, many times without your knowledge. Stalkers can intercept and monitor email using spyware or by getting your password; they might change your email settings so they can get secretly forwarded or secretly copied (designated as bcc) on every email you send or receive from that account.	▪ Avoid using email for sensitive or personal information. ▪ If you think your email is being monitored, consider creating an additional new email account on a safer computer. Never access the new accounts on a monitored computer (see above). ▪ When setting up a new email account, don't use any identifying information. ▪ Avoid passwords that others can guess. ▪ If you receive threats by email, save the electronic copies. Keep the emails in the system, but also consider forwarding a copy to another email account. You can also print copies of the email;

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

NNEDV

Technology Safety Quick Tips

Device	Description / Risks	Safety Strategies
		see if the print version can display the full email header. ▪ Consider reporting email threats or hacked accounts to law enforcement. These are crimes and the police can use email header information to help trace emails to the original sender.
Hidden Cameras	▪ Affordable, accessible, and easy to install, cameras come hidden in various items (clocks, plants, etc.). ▪ Can be wired into your house or transmit wirelessly. ▪ Can be very difficult to detect. ▪ Can create image files that include time, date and location data. ▪ Abuser can install camera surveillance and monitor all your activity remotely over the Internet.	▪ Trust instincts. If abuser knows something that can only be seen, a camera may be being used. ▪ Camera detectors can help to find wireless cameras that are giving off a signal, but will not detect a wired camera. ▪ Law enforcement may help to search for hidden cameras.
Personal Information & the Internet	▪ All kinds of public and private organizations, agencies, services, and businesses collect and share information about people. These can include government and nongovernmental organizations, community groups, schools and online sites such as social networking, gaming or job sites. Search engines index the web and create virtual card catalogs. Some search deep into online databases and compile extensive profiles on people. ▪ Identifying information may be online without victims' knowledge. ▪ Stalkers use the Internet to find information about the victim including the location and contact information of victim. They also use online spaces to defame, target and damage the reputation of the victim.	▪ Do searches on yourself to see what information is available. ▪ Be cautious and creative when providing personal information: only provide information that you feel is critical and safe for things like store discount cards. ▪ Ask schools, employers, courts and government services about Internet publications. Request that your information and photos not be posted in public directories or online. In court systems, ask up front how your court records can be sealed and not posted online for safety reasons. ▪ If you have a restraining order, providing that can expedite these requests.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

Who's Spying on Your Computer?

Spyware, Surveillance, and Safety for Survivors

Reprinted with permission The National Network to End Domestic Violence

SAFETY ALERT: Spyware has made it easier than ever before for perpetrators to stalk, track, monitor, and harass their victims. Abusers, stalkers, and other perpetrators can now use spyware to secretly monitor what you do on your computer or handheld device, like a cell phone. If you suspect you are being stalked or monitored, be aware that:

- Attempting to look for spyware on your computer or cellphone could be dangerous since the abuser could be alerted to your searches immediately.
- Use a safer computer (one that the stalker does not have remote or physical access) to perform Internet searches or send emails that you wouldn't want an abuser to intercept.

WHAT IS SPYWARE?

Spyware is a computer software program or hardware device that enables an unauthorized person (such as an abuser) to secretly monitor and gather information about your computer use.

There are many types of computer software programs and hardware devices that can be installed to monitor your computer activities. They can be installed on your computer without your knowledge, and the person installing them doesn't even need to have physical access to your computer. Spyware is invasive, intrusive, and may put victims in grave danger.

HOW DOES SPYWARE WORK?

Spyware can keep track of every keystroke you type, every software application you use, every website you visit, every chat or instant message you send, every document you open, and everything you print. Some spyware software gives the person monitoring the ability to freeze, shutdown or restart your computer. Some versions even allow the abuser to remotely turn on your webcam or make your computer talk.

Once spyware is installed, it can run in stealth mode and is difficult to detect or uninstall. If the person who installed it has physical access to your computer, he or she can log into the computer with a special password to see all of the computer activity (emails sent, documents printed, websites visited, and more) since their last log in. Perpetrators without physical access to your computer can receive reports showing all of your computer activities, including copies of emails and instant messages sent, websites visited, etc., as well as screenshots of the computer screen every few seconds. This can all occur without the user knowing.

Below are the computer activities that can be easily monitored:

Who's Spying on Your Computer?

Spyware, Surveillance, and Safety for Survivors

HOW DOES SPYWARE GET ON MY COMPUTER?

Abusers can install spyware on your computer if they have physical or Internet access to your computer. Some abusers might hack into your computer from another location via the Internet. Some might send spyware to you as an attached file that automatically installs itself when you open the email. Others may email or instant message a greeting card, computer game, or other ploy to entice you or your children to open an attachment or click on a link. Once opened, the program automatically installs spyware on the victim's computer, in stealth mode without notification or consent, and can then send electronic reports to the perpetrator via the Internet.

While most spyware is software based (a program that can be installed on your computer), there are also some hardware-based spyware devices called keystroke loggers. These keylogging devices may appear to be a normal computer part; for example, it can be a special keyboard with keystroke logging capabilities or a small device that connects your keyboard to the computer. Once the keylogger is plugged into your computer, it can record every key typed, capturing all passwords, personal identification numbers (PIN), websites visited, and any emails sent.

HOW DO I FIND OUT IF SPYWARE IS ON MY COMPUTER?

Even if a computer is being monitored by spyware, there may not be noticeable changes in the way your computer operates (i.e., your computer won't necessarily slow down or freeze up). You might suspect that your computer is being monitored by the abuser's suspicious behavior: for example, he or she knows too much about your computer activities. If you suspect that someone has installed spyware to monitor your activities, talk to a victim advocate before attempting to remove the spyware. Law enforcement or a computer forensics expert may be able to assist you if you want to preserve evidence that may be needed for a criminal investigation.

Unfortunately, detecting spyware on your computer may be difficult. If a hardware device has been installed, you might see an additional component between the computer and the keyboard cord, or it might be the keyboard or mouse itself. In laptops, hardware device would be installed inside the laptop, through the access panel. Hardware spyware cannot be detected by anti-spyware software.

Software spyware typically runs in stealth mode using disguised file names that look legitimate. Sometimes, running anti-spyware software may detect this type of spyware but not all of it.

TIPS FOR SURVIVORS

Trust your instincts and look for patterns. If your abuser knows too much about things you've only told people via email or instant messenger or things you've done on your computer, there may be spyware on your computer.

Supported by US DOJ-OVC Grant # 2011-VF-GX-K016. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

Who's Spying on Your Computer?

Spyware, Surveillance, and Safety for Survivors

Everything is being recorded. If you suspect your computer is being monitored, remember that all that you do, including research on spyware and computer monitoring, will be revealed to the abuser. Strategize around the safety concerns that may arise if the abuser thinks that you know and are attempting to remove their control. If you can, use a safer computer when you look for domestic or sexual violence resources. It may be safer to use a computer at a public library, community center, or internet café. Clearing or deleting your internet browsing history or deleting documents from your computer will not prevent the spyware from capturing what you're doing. The spyware will actually record everything you do, including attempts to clear your browsing history.

Create new accounts & change passwords. If you suspect that anyone abusive can access your email or Instant Messaging (IM), consider creating additional email/IM accounts on a safer computer. Do not create or check new email/IM accounts from a computer that might be monitored. Look for free web-based email accounts, and consider using non-identifying name and account information. (Example: bluecat@email.com and not YourRealName@email.com.) Also consider changing passwords to sensitive accounts such as online banks, social media accounts, etc. from a safer computer.

New software or hardware? Be suspicious if someone abusive has installed a new keyboard, cord, or software or updated or "fixed" the computer—particularly if this coincides with increased monitoring or stalking. Beware of gifts from the abuser to you or your children, such as new keyboards, cell phones, or games for the computer as it may contain spyware.

Preventive measures you can take: There are steps you can take to reduce the chance of spyware. Note that these suggestions will help prevent spyware from being installed and work best before your computer has been compromised.

- Install and enable a firewall. There are both software and hardware firewalls. If a firewall didn't come with your computer, you can download a software one for free from www.zonealarm.com.
- Have a anti-virus protection program installed. Make sure your anti-virus definitions are up-to-date because new dangerous viruses are released daily and that it scans your computer regularly. This may involve setting your computer to automatically update its virus definitions and run anti-virus scans daily. When your anti-virus software subscription ends, make sure to renew it.
- Install anti-spyware programs and make sure the spyware definitions are updated automatically and regularly.
- These programs will only protect you from spyware software or programs but not hardware devices, such as a keystroke logging keyboard or device.

Buy a new computer. It is almost impossible to completely delete, erase or uninstall spyware from your computer. The safest way to ensure that your computer is no longer being monitored is to purchase a new computer. Be careful about moving files (including software, documents, pictures, videos) from the infected computer to the clean computer as the spyware may reinstall onto the new computer.

Supported by US DOJ-OVC Grant # 2011-VF-GX-K016. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

Include the children and other family members. It is important for you and your children to be educated about spyware and to make sure that the kids don't inadvertently install spyware onto the computer. Talk to your children about opening emails from people they don't know or from opening attachments from the abusive person. An innocuous picture or video may be something that the child wants to see but can also contain spyware. Instead of sharing files and media via email between the abuser and you and the children, consider creating online spaces to share pictures, videos and documents. Some online spaces will allow you to create private spaces, so no one else can access it but authorized users.

Safety when removing spyware. Many abusers use spyware as a way to monitor and control survivors. Some abusers may escalate their control and monitoring if they suspect that the survivor is cutting off their access. Think through your safety as you consider ways to protect yourself.

Additional resource. For more information on avoiding and removing spyware from your computer, please see this document "Protecting Your Computer":
http://www.antispywarecoalition.org/documents/documents/ProtectingYourComputerflyerletter.pdf

Spyware for Cell Phones

Spyware programs are now available for cell phones and other handheld devices so perpetrators can track phone activities, including calls and texts that are sent or received, record conversations, and can even be used as a listening device. The abuser will need to have physical access to the phone to manually install the software onto the phone. If you suspect that your cell phone is being monitored, keep an eye on excessive battery or data usage and suspicious patterns of behavior from the abusive person. You can take steps to protect your phone by putting a passcode on your phone and running an anti-spyware/anti-malware app on your phone if your phone has that capability. *(Don't forget that some phone activities can be monitored without spyware. Phone records can be obtained by guessing your account password and accessing your account online or by viewing your call history stored in the phone.)*

Supported by US DOJ-OVC Grant # 2011-VF-GX-K016. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

NYCLA ETHICS OPINION 745
JULY 2, 2013

ADVISING A CLIENT REGARDING POSTS ON SOCIAL MEDIA SITES

TOPIC: What advice is appropriate to give a client with respect to existing or proposed postings on social media sites.

DIGEST: It is the Committee's opinion that New York attorneys may advise clients as to (1) what they should/should not post on social media, (2) what existing postings they may or may not remove, and (3) the particular implications of social media posts, subject to the same rules, concerns, and principles that apply to giving a client legal advice in other areas including RPC 3.1, 3.3 and 3.4.[1]

RPC: 4.1, 4.2, 3.1, 3.3, 3.4, 8.4.

OPINION:

This opinion provides guidance about how attorneys may advise clients concerning what may be posted or removed from social media websites. It has been estimated that Americans spend 20 percent of their free time on social media (Facebook, Twitter, Friendster, Flickr, LinkedIn, and the like). It is commonplace to post travel logs, photographs, streams of consciousness, rants, and all manner of things on websites so that family, friends, or even the public-at-large can peer into one's life. Social media enable users to publish information regionally, nationally, and even globally.

The personal nature of social media posts implicates considerable privacy concerns. Although all of the major social media outlets have password protections and various levels of privacy settings, many users are oblivious or indifferent to them, providing an opportunity for persons with adverse interests to learn even the most intimate information about them. For example, teenagers and college students commonly post photographs of themselves partying, binge drinking, indulging in illegal drugs or sexual poses, and the like. The posters may not be aware, or may not care, that these posts may find their way into the hands of family, potential employers, school admission officers, romantic contacts, and others. The content of a removed social media posting may continue to exist, on the poster's computer, or in cyberspace.

[1] This opinion is limited to conduct of attorneys in connection with civil matters. Attorneys involved in criminal cases may have different ethical responsibilities.

That information posted on social media may undermine a litigant's position has not been lost on attorneys. Rather than hire investigators to follow claimants with video cameras, personal injury defendants may seek to locate YouTube videos or Facebook photos that depict a "disabled" plaintiff engaging in activities that are inconsistent with the claimed injuries. It is now common for attorneys and their investigators to seek to scour litigants' social media pages for information and photographs. Demands for authorizations for access to password-protected portions of an opposing litigant's social media sites are becoming routine.

Recent ethics opinions have concluded that accessing a social media page open to all members of a public network is ethically permissible. New York State Bar Association Eth. Op. 843 (2010); Oregon State Bar Legal Ethics Comm., Op. 2005-164 (finding that accessing an opposing party's public website does not violate the ethics rules limiting communications with adverse parties). The reasoning behind these opinions is that accessing a public site is conceptually no different from reading a magazine article or purchasing a book written by that adverse party. Oregon Op. 2005-164 at 453.

But an attorney's ability to access social media information is not unlimited. Attorneys may not make misrepresentations to obtain information that would otherwise not be obtainable. In contact with victims, witnesses, or others involved in opposing counsel's case, attorneys should avoid misrepresentations, and, in the case of a represented party, obtain the prior consent of the party's counsel. New York Rules of Professional Conduct (RPC 4.2). See, NYCBA Eth. Op., 2010-2 (2012); NYSBA Eth. Op. 843. Using false or misleading representations to obtain evidence from a social network website is prohibited. RPC 4.1, 8.4(c).

Social media users may have some expectation of privacy in their posts, depending on the privacy settings available to them, and their use of those settings. All major social media allow members to set varying levels of security and "privacy" on their social media pages. There is no ethical constraint on advising a client to use the highest level of privacy/security settings that is available. Such settings will prevent adverse counsel from having direct access to the contents of the client's social media pages, requiring adverse counsel to request access through formal discovery channels.

A number of recent cases have considered the extent to which courts may direct litigants to authorize adverse counsel to access the "private" portions of their social media postings. While a comprehensive review of this evolving body of law is beyond the scope of this opinion, the premise behind such cases is that social media websites may contain materials inconsistent with a party's litigation posture, and thus may be used for impeachment. The newest cases turn on whether the party seeking such disclosure has laid a sufficient foundation that such impeachment material likely exists or whether the party is engaging in a "fishing expedition" and an invasion of privacy in the hopes of stumbling onto something that may be useful.[2]

[2] In Tapp v. N.Y.S. Urban Dev. Corp., 102 A.D.3d 620, 958 N.Y.S. 2d 392 (1st Dep't 2013), the First Department held that a defendant's contention that Facebook activities "may reveal daily activities that contradict or conflict with

Given the growing volume of litigation regarding social media discovery, the question arises whether an attorney may instruct a client who does not have a social media site not to create one: May an attorney pre-screen what a client posts on a social media site? May an attorney properly instruct a client to "take down" certain materials from an existing social media site?

Preliminarily, we note that an attorney's obligation to represent clients competently (RPC 1.1) could, in some circumstances, give rise to an obligation to advise clients, within legal and ethical requirements, concerning what steps to take to mitigate any adverse effects on the clients' position emanating from the clients' use of social media. Thus, an attorney may properly review a client's social media pages, and advise the client that certain materials posted on a social media page may be used against the client for impeachment or similar purposes. In advising a client, attorneys should be mindful of their ethical responsibilities under RPC 3.4. That rule provides that a lawyer shall not "(a)(1) suppress any evidence that the lawyer or the client has a legal obligation to reveal or produce... [nor] (3) conceal or knowingly fail to disclose that which the lawyer is required by law to reveal."

Attorneys' duties not to suppress or conceal evidence involve questions of substantive law and are therefore outside the purview of an ethics opinion. We do note, however, that applicable state or federal law may make it an offense to destroy material for the purpose of defeating its availability in a pending or reasonably foreseeable proceeding, even if no specific request to reveal or produce evidence has been made. Under principles of substantive law, there may be a duty to preserve "potential evidence" in advance of any request for its discovery. VOOM HD Holdings LLC v. EchoStar Satellite L.L.C., 93 A.D.3d 33, 939 N.Y.S. 2d 331 (1st Dep't 2012) ("Once a party reasonably anticipates litigation, it must, at a minimum, institute an appropriate litigation hold to prevent the routine destruction of electronic data."); QK Healthcare, Inc., v. Forest Laboratories, Inc., 2013 N.Y. Misc. LEXIS 2008; 2013 N.Y. Slip Op. 31028(U) (Sup. Ct. N.Y. Co., May 8, 2013); RPC 3.4, Comment [2]. Under some circumstances, where litigation is anticipated, a duty to preserve evidence may arise under substantive law. But provided that such removal does not violate the substantive law regarding destruction or spoliation of evidence, there is no ethical bar to "taking down" such material from social media publications, or prohibiting a client's attorney from advising the client to do so, particularly inasmuch as the substance of the posting is generally preserved in cyberspace or on the user's computer.

An attorney also has an ethical obligation not to "bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis in law and fact for doing so that is not frivolous."

---

plaintiff's" claim isn't enough. "Mere possession and utilization of a Facebook account is an insufficient basis to compel plaintiff to provide access to the account or to have the court conduct an in camera inspection of the account's usage. To warrant discovery, defendants must establish a factual predicate for their request by identifying relevant information in plaintiff's Facebook account — that is, information that 'contradicts or conflicts with plaintiff's alleged restrictions, disabilities, and losses, and other claims.'" Also, see, Kregg v. Maldonado, 98 A.D.3d 1289, 951 N.Y.S. 2d 301 (4th Dep't 2012); Patterson v. Turner Constr. Co., 88 A.D.3d 617, 931 N.Y.S. 2d 311 (1st Dep't 2011); McCann v. Harleysville Ins. Co. of N.Y., 78 A.D.3d 1524, 910 N.Y.S. 2d 614 (4th Dep't 2010).

RPC 3.1(a). Frivolous conduct includes the knowing assertion of "material factual statements that are false." RPC 3.1(b)(3). Therefore, if a client's social media posting reveals to an attorney that the client's lawsuit involves the assertion of material false factual statements, and if proper inquiry of the client does not negate that conclusion, the attorney is ethically prohibited from proffering, supporting or using those false statements. See, also, RPC 3.3; 4.1 ("In the course of representing a client, a lawyer shall not knowingly make a false statement of fact or law to a third person.")

Clients are required to testify truthfully at a hearing, deposition, trial, or the like, and a lawyer may not fail to correct a false statement of material fact or offer or use evidence the lawyer knows to be false. RPC 3.3(a)(1); 3.4(a)(4). Thus, a client must answer truthfully (subject to the rules of privilege or other evidentiary objections) if asked whether changes were ever made to a social media site, and the client's lawyer must take prompt remedial action in the case of any known material false testimony on this subject. RPC 3.3 (a)(3).

We further conclude that it is permissible for an attorney to review what a client plans to publish on a social media page in advance of publication, to guide the client appropriately, including formulating a corporate policy on social media usage. Again, the above ethical rules and principles apply: An attorney may not direct or facilitate the client's publishing of false or misleading information that may be relevant to a claim; an attorney may not participate in the creation or preservation of evidence when the lawyer knows or it is obvious that the evidence is false. RPC 3.4(a)(4).[3] However, a lawyer may counsel the witness to publish truthful information favorable to the lawyer's client; discuss the significance and implications of social media posts (including their content and advisability); advise the client how social media posts may be received and/or presented by the client's legal adversaries and advise the client to consider the posts in that light; discuss the possibility that the legal adversary may obtain access to "private" social media pages through court orders or compulsory process; review how the factual context of the posts may affect their perception; review the posts that may be published and those that have already been published; and discuss possible lines of cross-examination.

CONCLUSION:

Lawyers should comply with their ethical duties in dealing with clients' social media posts. The ethical rules and concepts of fairness to opposing counsel and the court, under RPC 3.3 and 3.4, all apply. An attorney may advise clients to keep their social media privacy settings turned on or maximized and may advise clients as to what should or should not be posted on public and/or private pages, consistent with the principles stated above. Provided that there is no violation of the rules or substantive law pertaining to the preservation and/or spoliation of evidence, an attorney may offer advice as to what may be kept on "private" social media pages, and what may be "taken down" or removed.

[3] We do not suggest that all information on Facebook pages would constitute admissible evidence; such determinations must be made as a matter of substantive law on a case by case basis.

THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK
COMMITTEE ON PROFESSIONAL ETHICS

FORMAL OPINION 2010-2

OBTAINING EVIDENCE FROM SOCIAL NETWORKING WEBSITES

TOPIC: Lawyers obtaining information from social networking websites.

DIGEST: A lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent.

RULES: 4.1(a), 5.3(c)(1), 8.4(a) & (c)

QUESTION: May a lawyer, either directly or through an agent, contact an unrepresented person through a social networking website and request permission to access her web page to obtain information for use in litigation?

OPINION

Lawyers increasingly have turned to social networking sites, such as Facebook, Twitter and YouTube, as potential sources of evidence for use in litigation.[1] In light of the information regularly found on these sites, it is not difficult to envision a matrimonial matter in which allegations of infidelity may be substantiated in whole or part by postings on a Facebook wall.[2] Nor is it hard to imagine a copyright infringement case that turns largely on the postings of certain allegedly pirated videos on YouTube. The potential availability of helpful evidence on these internet-based sources makes them an attractive new weapon in a lawyer's arsenal of formal and informal discovery devices.[3] The prevalence of these and other social networking websites, and the potential

[1] Social networks are internet-based communities that individuals use to communicate with each other and view and exchange information, including photographs, digital recordings and files. Users create a profile page with personal information that other users may access online. Users may establish the level of privacy they wish to employ and may limit those who view their profile page to "friends" – those who have specifically sent a computerized request to view their profile page which the user has accepted. Examples of currently popular social networks include Facebook, Twitter, MySpace and LinkedIn.

[2] See, e.g., Stephanie Chen, Divorce attorneys catching cheaters on Facebook, June 1, 2010, http://www.cnn.com/2010/TECH/social.media/06/01/facebook.divorce.lawyers/index.html?hpt=C2.

[3] See, e.g., Bass ex rel. Bass v. Miss Porter's School, No. 3:08cv01807, 2009 WL 3724968, at *1-2 (D. Conn. Oct. 27, 2009).

benefits of accessing them to obtain evidence, present ethical challenges for attorneys navigating these virtual worlds.

In this opinion, we address the narrow question of whether a lawyer, acting either alone or through an agent such as a private investigator, may resort to trickery via the internet to gain access to an otherwise secure social networking page and the potentially helpful information it holds. In particular, we focus on an attorney's direct or indirect use of affirmatively "deceptive" behavior to "friend" potential witnesses. We do so in light of, among other things, the Court of Appeals' oft-cited policy in favor of informal discovery. See, e.g., Niesig v. Team I, 76 N.Y.2d 363, 372, 559 N.Y.S.2d 493, 497 (1990) ("[T]he Appellate Division's blanket rule closes off avenues of informal discovery of information that may serve both the litigants and the entire justice system by uncovering relevant facts, thus promoting the expeditious resolution of disputes."); Muriel, Siebert & Co. v. Intuit Inc., 8 N.Y.3d 506, 511, 836 N.Y.S.2d 527, 530 (2007) ("the importance of informal discovery underlies our holding here"). It would be inconsistent with this policy to flatly prohibit lawyers from engaging in any and all contact with users of social networking sites. Consistent with the policy, we conclude that an attorney or her agent may use her real name and profile to send a "friend request" to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request.[4] While there are ethical boundaries to such "friending," in our view they are not crossed when an attorney or investigator uses only truthful information to obtain access to a website, subject to compliance with all other ethical requirements. See, e.g., id., 8 N.Y.3d at 512, 836 N.Y.S.2d at 530 ("Counsel must still conform to all applicable ethical standards when conducting such [ex parte] interviews [with opposing party's former employee]." (citations omitted)).

The potential ethical pitfalls associated with social networking sites arise in part from the informality of communications on the web. In that connection, in seeking access to an individual's personal information, it may be easier to deceive an individual in the virtual world than in the real world. For example, if a stranger made an unsolicited face-to-face request to a potential witness for permission to enter the witness's home, view the witness's photographs and video files, learn the witness's relationship status, religious views and date of birth, and review the witness's personal diary, the witness almost certainly would slam the door shut and perhaps even call the police.

In contrast, in the "virtual" world, the same stranger is more likely to be able to gain admission to an individual's personal webpage and have unfettered access to most, if not all, of the foregoing information. Using publicly-available information, an attorney or her investigator could easily create a false Facebook profile listing schools, hobbies,

[4] The communications of a lawyer and her agents with parties known to be represented by counsel are governed by Rule 4.2, which prohibits such communications unless the prior consent of the party's lawyer is obtained or the conduct is authorized by law. N.Y. Prof'l Conduct R. 4.2. The term "party" is generally interpreted broadly to include "represented witnesses, potential witnesses and others with an interest or right at stake, although they are not nominal parties." N.Y. State 735 (2001). Cf. N.Y. State 843 (2010)(lawyers may access public pages of social networking websites maintained by any person, including represented parties).

interests, or other background information likely to be of interest to a targeted witness. After creating the profile, the attorney or investigator could use it to make a "friend request" falsely portraying the attorney or investigator as the witness's long lost classmate, prospective employer, or friend of a friend. Many casual social network users might accept such a "friend request" or even one less tailored to the background and interests of the witness. Similarly, an investigator could e-mail a YouTube account holder, falsely touting a recent digital posting of potential interest as a hook to ask to subscribe to the account holder's "channel" and view all of her digital postings. By making the "friend request" or a request for access to a YouTube "channel," the investigator could obtain instant access to everything the user has posted and will post in the future. In each of these instances, the "virtual" inquiries likely have a much greater chance of success than if the attorney or investigator made them in person and faced the prospect of follow-up questions regarding her identity and intentions. The protocol on-line, however, is more limited both in substance and in practice. Despite the common sense admonition not to "open the door" to strangers, social networking users often do just that with a click of the mouse.

Under the New York Rules of Professional Conduct (the "Rules"), an attorney and those in her employ are prohibited from engaging in this type of conduct. The applicable restrictions are found in Rules 4.1 and 8.4(c). The latter provides that "[a] lawyer or law firm shall not . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation." N.Y. Prof'l Conduct R. 8.4(c) (2010). And Rule 4.1 states that "[i]n the course of representing a client, a lawyer shall not knowingly make a false statement of fact or law to a third person." Id. 4.1. We believe these Rules are violated whenever an attorney "friends" an individual under false pretenses to obtain evidence from a social networking website.

For purposes of this analysis, it does not matter whether the lawyer employs an agent, such as an investigator, to engage in the ruse. As provided by Rule 8.4(a), "[a] lawyer or law firm shall not . . . violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another." Id. 8.4(a). Consequently, absent some exception to the Rules, a lawyer's investigator or other agent also may not use deception to obtain information from the user of a social networking website. See id. Rule 5.3(b)(1) ("A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if . . . the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it . . . .").

We are aware of ethics opinions that find that deception may be permissible in rare instances when it appears that no other option is available to obtain key evidence. See N.Y. County 737 (2007) (requiring, for use of dissemblance, that "the evidence sought is not reasonably and readily obtainable through other lawful means"); see also ABCNY Formal Op. 2003-02 (justifying limited use of undisclosed taping of telephone conversations to achieve a greater societal good where evidence would not otherwise be available if lawyer disclosed taping). Whatever the utility and ethical grounding of these limited exceptions -- a question we do not address here -- they are, at least in

most situations, inapplicable to social networking websites. Because non-deceptive means of communication ordinarily are available to obtain information on a social networking page -- through ordinary discovery of the targeted individual or of the social networking sites themselves -- trickery cannot be justified as a necessary last resort.[5] For this reason we conclude that lawyers may not use or cause others to use deception in this context.

Rather than engage in "trickery," lawyers can -- and should -- seek information maintained on social networking sites, such as Facebook, by availing themselves of informal discovery, such as the truthful "friending" of unrepresented parties, or by using formal discovery devices such as subpoenas directed to non-parties in possession of information maintained on an individual's social networking page. Given the availability of these legitimate discovery methods, there is and can be no justification for permitting the use of deception to obtain the information from a witness on-line.[6]

Accordingly, a lawyer may not use deception to access information from a social networking webpage. Rather, a lawyer should rely on the informal and formal discovery procedures sanctioned by the ethical rules and case law to obtain relevant evidence.

September 2010

[5] Although a question of law beyond the scope of our reach, the Stored Communications Act, 18 U.S.C. § 2701(a)(1) et seq. and the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq., among others, raise questions as to whether certain information is discoverable directly from third-party service providers such as Facebook. Counsel, of course, must ensure that her contemplated discovery comports with applicable law.

[6] While we recognize the importance of informal discovery, we believe a lawyer or her agent crosses an ethical line when she falsely identifies herself in a "friend request". See, e.g., Niesig v. Team I, 76 N.Y.2d 363, 376, 559 N.Y.S.2d 493, 499 (1990) (permitting ex parte communications with certain employees); Muriel Siebert, 8 N.Y.3d at 511, 836 N.Y.S.2d at 530 ("[T]he importance of informal discovery underlie[s] our holding here that, so long as measures are taken to steer clear of privileged or confidential information, adversary counsel may conduct ex parte interviews of an opposing party's former employee.").

NEW YORK STATE BAR ASSOCIATION
Committee on Professional Ethics

Opinion 843 (9/10/10)

Topic: Lawyer's access to public pages of another party's social networking site for the purpose of gathering information for client in pending litigation.

Digest: A lawyer representing a client in pending litigation may access the public pages of another party's social networking website (such as Facebook or MySpace) for the purpose of obtaining possible impeachment material for use in the litigation.

Rules: 4.1; 4.2; 4.3; 5.3(b)(1); 8.4(c)

QUESTION

1. May a lawyer view and access the Facebook or MySpace pages of a party other than his or her client in pending litigation in order to secure information about that party for use in the lawsuit, including impeachment material, if the lawyer does not "friend" the party and instead relies on public pages posted by the party that are accessible to all members in the network?

OPINION

2. Social networking services such as Facebook and MySpace allow users to create an online profile that may be accessed by other network members. Facebook and MySpace are examples of external social networks that are available to all web users. An external social network may be generic (like MySpace and Facebook) or may be formed around a specific profession or area of interest. Users are able to upload pictures and create profiles of themselves. Users may also link with other users, which is called "friending." Typically, these social networks have privacy controls that allow users to choose who can view their profiles or contact them; both users must confirm that they wish to "friend" before they are linked and can view one another's profiles. However, some social networking sites and/or users do not require pre-approval to gain access to member profiles.

3. The question posed here has not been addressed previously by an ethics committee interpreting New York's Rules of Professional Conduct (the "Rules") or the former New York Lawyers Code of Professional Responsibility, but some guidance is available from outside New York. The Philadelphia Bar Association's Professional Guidance Committee recently analyzed the propriety of "friending" an unrepresented adverse witness in a pending lawsuit to obtain potential impeachment material. See Philadelphia Bar Op. 2009-02 (March 2009). In that opinion, a lawyer asked whether she could cause a third party to access the Facebook and MySpace pages maintained by a witness to obtain information that might be useful for impeaching the witness at trial. The witness's Facebook and MySpace pages were not generally accessible to the public, but rather were accessible only with the witness's permission (*i.e.,* only when the witness allowed someone to "friend" her). The inquiring lawyer proposed to have the third party "friend" the witness to access the witness's Facebook and MySpace accounts and provide truthful information about the third party, but conceal the association with the lawyer and the real purpose behind "friending" the witness (obtaining potential impeachment material).

4. The Philadelphia Professional Guidance Committee, applying the Pennsylvania Rules of Professional Conduct, concluded that the inquiring lawyer could not ethically engage in the proposed conduct. The lawyer's intention to have a third party "friend" the unrepresented witness implicated Pennsylvania Rule 8.4(c) (which, like New York's Rule 8.4(c), prohibits a lawyer from engaging in conduct involving "dishonesty, fraud, deceit or misrepresentation"); Pennsylvania Rule

5.3(c)(1) (which, like New York's Rule 5.3(b)(1), holds a lawyer responsible for the conduct of a nonlawyer employed by the lawyer if the lawyer directs, or with knowledge ratifies, conduct that would violate the Rules if engaged in by the lawyer); and Pennsylvania Rule 4.1 (which, similar to New York's Rule 4.1, prohibits a lawyer from making a false statement of fact or law to a third person). Specifically, the Philadelphia Committee determined that the proposed "friending" by a third party would constitute deception in violation of Rules 8.4 and 4.1, and would constitute a supervisory violation under Rule 5.3 because the third party would omit a material fact (*i.e.,* that the third party would be seeking access to the witness's social networking pages solely to obtain information for the lawyer to use in the pending lawsuit).

5. Here, in contrast, the Facebook and MySpace sites the lawyer wishes to view are accessible to all members of the network. New York's Rule 8.4 would not be implicated because the lawyer is not engaging in deception by accessing a public website that is available to anyone in the network, provided that the lawyer does not employ deception in any other way (including, for example, employing deception to become a member of the network). Obtaining information about a party available in the Facebook or MySpace profile is similar to obtaining information that is available in publicly accessible online or print media, or through a subscription research service such as Nexis or Factiva, and that is plainly permitted.[1] Accordingly, we conclude that the lawyer may ethically view and access the Facebook and MySpace profiles of a party other than the lawyer's client in litigation as long as the party's profile is available to all members in the network and the lawyer neither "friends" the other party nor directs someone else to do so.

CONCLUSION

6. A lawyer who represents a client in a pending litigation, and who has access to the Facebook or MySpace network used by another party in litigation, may access and review the public social network pages of that party to search for potential impeachment material. As long as the lawyer does not "friend" the other party or direct a third person to do so, accessing the social network pages of the party will not violate Rule 8.4 (prohibiting deceptive or misleading conduct), Rule 4.1 (prohibiting false statements of fact or law), or Rule 5.3(b)(1) (imposing responsibility on lawyers for unethical conduct by nonlawyers acting at their direction).

(76-09)

---

[1] One of several key distinctions between the scenario discussed in the Philadelphia opinion and this opinion is that the Philadelphia opinion concerned an unrepresented *witness*, whereas our opinion concerns a *party* – and this party may or may not be represented by counsel in the litigation. If a lawyer attempts to "friend" a *represented* party in a pending litigation, then the lawyer's conduct is governed by Rule 4.2 (the "no-contact" rule), which prohibits a lawyer from communicating with the represented party about the subject of the representation absent prior consent from the represented party's lawyer. If the lawyer attempts to "friend" an *unrepresented* party, then the lawyer's conduct is governed by Rule 4.3, which prohibits a lawyer from stating or implying that he or she is disinterested, requires the lawyer to correct any misunderstanding as to the lawyer's role, and prohibits the lawyer from giving legal advice other than the advice to secure counsel if the other party's interests are likely to conflict with those of the lawyer's client.Our opinion does not address these scenarios.

COMMITTEE REPORT

Formal Opinion 2012-2 - Jury Research and Social Media

May 30, 2012

TOPIC: Jury Research and Social Media

DIGEST: Attorneys may use social media websites for juror research as long as no communication occurs between the lawyer and the juror as a result of the research. Attorneys may not research jurors if the result of the research is that the juror will receive a communication. If an attorney unknowingly or inadvertently causes a communication with a juror, such conduct may run afoul of the Rules of Professional Conduct. The attorney must not use deception to gain access to a juror's website or to obtain information, and third parties working for the benefit of or on behalf of an attorney must comport with all the same restrictions as the attorney. Should a lawyer learn of juror misconduct through otherwise permissible research of a juror's social media activities, the lawyer must reveal the improper conduct to the court.

RULES: 3.5(a)(4); 3.5(a)(5); 3.5(d); 8.4

Question: What ethical restrictions, if any, apply to an attorney's use of social media websites to research potential or sitting jurors?

OPINION

I. Introduction

Ex parte attorney communication with prospective jurors and members of a sitting jury has long been prohibited by state rules of professional conduct (see American Bar Association Formal Opinion 319 ("ABA 319")), and attorneys have long sought ways to gather information about potential jurors during voir dire (and perhaps during trial) within these proscribed bounds. However, as the internet and social media have changed the ways in which we all communicate, conducting juror research while complying with the rule prohibiting juror communication has become more complicated.

In addition, the internet appears to have increased the opportunity for juror misconduct, and attorneys are responding by researching not only members of the venire but sitting jurors as well. Juror misconduct over the internet is problematic and has even led to mistrials. Jurors have begun to use social media services as a platform to communicate about a trial, during the trial (see WSJ Law Blog (March 12, 2012), http://blogs.wsj.com/law/2012/03/12/jury-files-the-temptation-of-twitter/), and jurors also turn to the internet to conduct their own out of court research. For example, the Vermont Supreme Court recently overturned a child sexual assault conviction because a juror conducted his own research on the cultural significance of the alleged crime in Somali Bantu culture. State v. Abdi, No. 2012-255, 2012 WL 231555 (Vt. Jan. 26, 2012). In a case in Arkansas, a murder conviction was overturned because a juror tweeted during the trial, and in a Maryland corruption trial in 2009, jurors used Facebook to discuss their views of the case before deliberations. (Juror's Tweets Upend Trials, Wall

Street Journal, March 2, 2012.) Courts have responded in various ways to this problem. Some judges have held jurors in contempt or declared mistrials (see id.) and other courts now include jury instructions on juror use of the internet. (See New York Pattern Jury Instructions, Section III, infra.)However, 79% of judges who responded to a Federal Judicial Center survey admitted that "they had no way of knowing whether jurors had violated a social-media ban." (Juror's Tweets, supra.) In this context, attorneys have also taken it upon themselves to monitor jurors throughout a trial.

Just as the internet and social media appear to facilitate juror misconduct, the same tools have expanded an attorney's ability to conduct research on potential and sitting jurors, and clients now often expect that attorneys will conduct such research. Indeed, standards of competence and diligence may require doing everything reasonably possible to learn about the jurors who will sit in judgment on a case. However, social media services and websites can blur the line between independent, private research and interactive, interpersonal "communication." Currently, there are no clear rules for conscientious attorneys to follow in order to both diligently represent their clients and to abide by applicable ethical obligations. This opinion applies the New York Rules of Professional Conduct (the "Rules"), specifically Rule 3.5, to juror research in the internet context, and particularly to research using social networking services and websites.1

The Committee believes that the principal interpretive issue is what constitutes a "communication" under Rule 3.5. We conclude that if a juror were to (i) receive a "friend" request (or similar invitation to share information on a social network site) as a result of an attorney's research, or (ii) otherwise to learn of the attorney's viewing or attempted viewing of the juror's pages, posts, or comments, that would constitute a prohibited communication if the attorney was aware that her actions would cause the juror to receive such message or notification. We further conclude that the same attempts to research the juror might constitute a prohibited communication even if inadvertent or unintended. In addition, the attorney must not use deception—such as pretending to be someone else—to gain access to information about a juror that would otherwise be unavailable. Third parties working for the benefit of or on behalf of an attorney must comport with these same restrictions (as it is always unethical pursuant to Rule 8.4 for an attorney to attempt to avoid the Rule by having a non-lawyer do what she cannot). Finally, if a lawyer learns of juror misconduct through a juror's social media activities, the lawyer must promptly reveal the improper conduct to the court.

II. Analysis Of Ethical Issues Relevant To Juror Research

A. Prior Authority Regarding An Attorney's Ability To Conduct Juror Research Over Social Networking Websites

Prior ethics and judicial opinions provide some guidance as to what is permitted and prohibited in social media juror research. First, it should be noted that lawyers have long tried to learn as much as possible about potential jurors using various methods of information gathering permitted by courts, including checking and verifying voir dire answers. Lawyers have even been chastised for not conducting such research on potential jurors. For example, in a recent Missouri case, a juror failed to disclose her prior litigation history in response to a voir dire question. After a verdict was rendered, plaintiff's counsel

investigated the juror's civil litigation history using Missouri's automated case record service and found that the juror had failed to disclosure that she was previously a defendant in several debt collection cases and a personal injury action.2 Although the court upheld plaintiff's request for a new trial based on juror nondisclosure, the court noted that "in light of advances in technology allowing greater access to information that can inform a trial court about the past litigation history of venire members, it is appropriate to place a greater burden on the parties to bring such matters to the court's attention at an earlier stage." Johnson v. McCullough, 306 S.W.3d 551, 558-59 (Mo. 2010). The court also stated that "litigants should endeavor to prevent retrials by completing an early investigation." Id.at 559.

Similarly, the Superior Court of New Jersey recently held that a trial judge "acted unreasonably" by preventing plaintiff's counsel from using the internet to research potential jurors during voir dire. During jury selection in a medical malpractice case, plaintiff's counsel began using a laptop computer to obtain information on prospective jurors. Defense counsel objected, and the trial judge held that plaintiff's attorney could not use her laptop during jury selection because she gave no notice of her intent to conduct internet research during selection. Although the Superior Court found that the trial court's ruling was not prejudicial, the Superior Court stated that "there was no suggestion that counsel's use of the computer was in any way disruptive. That he had the foresight to bring his laptop computer to court, and defense counsel did not, simply cannot serve as a basis for judicial intervention in the name of 'fairness' or maintaining 'a level playing field.' The 'playing field' was, in fact, already 'level' because internet access was open to both counsel." Carino v. Muenzen, A-5491-08T1, 2010 N.J. Super. Unpub. LEXIS 2154, at *27 (N.J. Sup. Ct. App. Div. Aug. 30, 2010).3

Other recent ethics opinions have also generally discussed attorney research in the social media context. For example, San Diego County Bar Legal Ethics Opinion 2011-2 ("SDCBA 2011-2") examined whether an attorney can send a "friend request" to a represented party. SDCBA 2011-2 found that because an attorney must make a decision to "friend" a party, even if the "friend request [is] nominally generated by Facebook and not the attorney, [the request] is at least an indirect communication" and is therefore prohibited by the rule against ex parte communications with represented parties.4 In addition, the New York State Bar Association ("NYSBA") found that obtaining information from an adverse party's social networking personal webpage, which is accessible to all website users, "is similar to obtaining information that is available in publicly accessible online or print media, or through a subscription research service as Niexi or Factiva and that is plainly permitted." (NYSBA Opinion 843 at 2) (emphasis added).

And most recently, the New York County Lawyers' Association ("NYCLA") published a formal opinion on the ethics of conducting juror research using social media. NYCLA Formal Opinion 743 ("NYCLA 743") examined whether a lawyer may conduct juror research during voir dire and trial using Twitter, Facebook and other similar social networking sites. NYCLA 743 found that it is "proper and ethical under Rule 3.5 for a lawyer to undertake a pretrial search of a prospective juror's social networking site, provided there is no contact or communication with the prospective juror and the lawyer does not seek to 'friend' jurors, subscribe to their Twitter accounts, send jurors tweets or otherwise contact them. During the evidentiary or deliberation phases of a trial, a lawyer may visit the publicly available Twitter, Facebook or other social networking site of a juror but must not 'friend' the juror, email, send tweets or

otherwise communicate in any way with the juror or act in any way by which the juror becomes aware of the monitoring." (NYCLA 743 at 4.) The opinion further noted the importance of reporting to the court any juror misconduct uncovered by such research and found that an attorney must notify the court of any impropriety "before taking any further significant action in the case." Id. NYCLA concluded that attorneys cannot use knowledge of juror misconduct to their advantage but rather must notify the court.

As set forth below, we largely agree with our colleagues at NYCLA. However, despite the guidance of the opinions discussed above, the question at the core of applying Rule 3.5 to social media—what constitutes a communication—has not been specifically addressed, and the Committee therefore analyzes this question below.

B. An Attorney May Conduct Juror Research Using Social Media Services And Websites But Cannot Engage In Communication With A Juror

1. Discussion of Features of Various Potential Research Websites

Given the popularity and widespread usage of social media services, other websites and general search engines, it has become common for lawyers to use the internet as a tool to research members of the jury venire in preparation for jury selection as well as to monitor jurors throughout the trial. Whether research conducted through a particular service will constitute a prohibited communication under the Rules may depend in part on, among other things, the technology, privacy settings and mechanics of each service.

The use of search engines for research is already ubiquitous. As social media services have grown in popularity, they have become additional sources to research potential jurors. As we discuss below, the central question an attorney must answer before engaging in jury research on a particular site or using a particular service is whether her actions will cause the juror to learn of the research. However, the functionality, policies and features of social media services change often, and any description of a particular website may well become obsolete quickly. Rather than attempt to catalog all existing social media services and their ever-changing offerings, policies and limitations, the Committee adopts a functional definition.5

We understand "social media" to be services or websites people join voluntarily in order to interact, communicate, or stay in touch with a group of users, sometimes called a "network." Most such services allow users to create personal profiles, and some allow users to post pictures and messages about their daily lives. Professional networking sites have also become popular. The amount of information that users can view about each other depends on the particular service and also each user's chosen privacy settings. The information the service communicates or makes available to visitors as well as members also varies. Indeed, some services may automatically notify a user when her profile has been viewed, while others provide notification only if another user initiates an interaction. Because of the differences from service to service and the high rate of change, the Committee believes that it is an attorney's duty to research and understand the properties of the service or website she wishes to use for jury research in order to avoid inadvertent communications.

2. What Constitutes a “Communication”?

Any research conducted by an attorney into a juror or member of the venire’s background or behavior is governed in part by Rule 3.5(a)(4), which states: “a lawyer shall not . . . (4) communicate or cause another to communicate with a member of the jury venire from which the jury will be selected for the trial of a case or, during the trial of a case, with any member of the jury unless authorized to do so by law or court order.” The Rule does not contain a mens rea requirement; by its literal terms, it prohibits all communication, even if inadvertent. Because of this, the application of Rule 3.5(a)(4) to juror research conducted over the internet via social media services is potentially more complicated than traditional juror communication issues. Even though the attorney’s purpose may not be to communicate with a juror, but simply to gather information, social media services are often designed for the very purpose of communication, and automatic features or user settings may cause a “communication” to occur even if the attorney does intend not for one to happen or know that one may happen. This raises several ethical questions: is every visit to a juror’s social media website considered a communication? Should the intent to research, not to communicate, be the controlling factor? What are the consequences of an inadvertent or unintended communications? The Committee begins its analysis by considering the meaning of “communicate” and “communication,” which are not defined either in the Rule or the American Bar Association Model Rules.6

Black’s Law Dictionary (9th Ed.) defines “communication” as: “1. The expression or exchange of information by speech, writing, gestures, or conduct; the process of bringing an idea to another's perception. 2. The information so expressed or exchanged.” The Oxford English Dictionary defines “communicate” as: “To impart (information, knowledge, or the like) (to a person; also formerly with); to impart the knowledge or idea of (something), to inform a person of; to convey, express; to give an impression of, put across.” Similarly, Local Rule 26.3 of the United States District Courts for the Southern and Eastern Districts of New York defines “communication” (for the purposes of discovery requests) as: “the transmittal of information (in the form of facts, ideas, inquiries or otherwise).”

Under the above definitions, whether the communicator intends to “impart” a message or knowledge is seemingly irrelevant; the focus is on the effect on the receiver. It is the “transmission of,” “exchange of” or “process of bringing” information or ideas from one person to another that defines a communication. In the realm of social media, this focus on the transmission of information or knowledge is critical. A request or notification transmitted through a social media service may constitute a communication even if it is technically generated by the service rather than the attorney, is not accepted, is ignored, or consists of nothing more than an automated message of which the “sender” was unaware. In each case, at a minimum, the researcher imparted to the person being researched the knowledge that he or she is being investigated.

3. An Attorney May Research A Juror Through Social Media Websites As Long As No Communication Occurs

The Committee concludes that attorneys may use search engines and social media services to research potential and sitting jurors without violating the Rules, as long as no communication with the juror

occurs. The Committee notes that Rule 3.5(a)(4) does not impose a requirement that a communication be willful or made with knowledge to be prohibited. In the social media context, due to the nature of the services, unintentional communications with a member of the jury venire or the jury pose a particular risk. For example, if an attorney views a juror's social media page and the juror receives an automated message from the social media service that a potential contact has viewed her profile—even if the attorney has not requested the sending of that message or is entirely unaware of it—the attorney has arguably "communicated" with the juror. The transmission of the information that the attorney viewed the juror's page is a communication that may be attributable to the lawyer, and even such minimal contact raises the specter of the improper influence and/or intimidation that the Rules are intended to prevent. Furthermore, attorneys cannot evade the ethics rules and avoid improper influence simply by having a non-attorney with a name unrecognizable to the juror initiate communication, as such action will run afoul of Rule 8.4 as discussed in Section II(C), infra.

Although the text of Rule 3.5(a)(4) would appear to make any "communication"—even one made inadvertently or unknowingly—a violation, the Committee takes no position on whether such an inadvertent communication would in fact be a violation of the Rules. Rather, the Committee believes it is incumbent upon the attorney to understand the functionality of any social media service she intends to use for juror research. If an attorney cannot ascertain the functionality of a website, the attorney must proceed with great caution in conducting research on that particular site, and should keep in mind the possibility that even an accidental, automated notice to the juror could be considered a violation of Rule 3.5.

More specifically, and based on the Committee's current understanding of relevant services, search engine websites may be used freely for juror research because there are no interactive functions that could allow jurors to learn of the attorney's research or actions. However, other services may be more difficult to navigate depending on their functionality and each user's particular privacy settings. Therefore, attorneys may be able to do some research on certain sites but cannot use all aspects of the sites' social functionality. An attorney may not, for example, send a chat, message or "friend request" to a member of the jury or venire, or take any other action that will transmit information to the juror because, if the potential juror learns that the attorney seeks access to her personal information then she has received a communication. Similarly, an attorney may read any publicly-available postings of the juror but must not sign up to receive new postings as they are generated. Finally, research using services that may, even unbeknownst to the attorney, generate a message or allow a person to determine that their webpage has been visited may pose an ethical risk even if the attorney did not intend or know that such a "communication" would be generated by the website.

The Committee also emphasizes that the above applications of Rule 3.5 are meant as examples only. The technology, usage and privacy settings of various services will likely change, potentially dramatically, over time. The settings and policies may also be partially under the control of the person being researched, and may not be apparent, or even capable of being ascertained. In order to comply with the Rules, an attorney must therefore be aware of how the relevant social media service works, and of the limitations of her knowledge. It is the duty of the attorney to understand the functionality and privacy

settings of any service she wishes to utilize for research, and to be aware of any changes in the platforms' settings or policies to ensure that no communication is received by a juror or venire member.

C. An Attorney May Not Engage in Deception or Misrepresentation In Researching Jurors On Social Media Websites

Rule 8.4(c), which governs all attorney conduct, prohibits deception and misrepresentation.7 In the jury research context, this rule prohibits attorneys from, for instance, misrepresenting their identity during online communications in order to access otherwise unavailable information, including misrepresenting the attorney's associations or membership in a network or group in order to access a juror's information. Thus, for example, an attorney may not claim to be an alumnus of a school that she did not attend in order to view a juror's personal webpage that is accessible only to members of a certain alumni network.

Furthermore, an attorney may not use a third party to do what she could not otherwise do. Rule 8.4(a) prohibits an attorney from violating any Rule "through the acts of another." Using a third party to communicate with a juror is deception and violates Rule 8.4(c), as well as Rule 8.4(a), even if the third party provides the potential juror only with truthful information. The attorney violates both rules whether she instructs the third party to communicate via a social network or whether the third party takes it upon herself to communicate with a member of the jury or venire for the attorney's benefit. On this issue, the Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02 ("PBA 2009-02") concluded that if an attorney uses a third party to "friend" a witness in order to access information, she is guilty of deception because "[this action] omits a highly material fact, namely, that the third party who asks to be allowed access to the witness' pages is doing so only because she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit." (PBA 2009-02 at 3.) New York City Bar Association Formal Opinion 2010-2 similarly held that a lawyer may not gain access to a social networking website under false pretenses, either directly or through an agent, and NYCLA 743 also noted that Rule 8.4 governs juror research and an attorney therefore cannot use deception to gain access to a network or direct anyone else to "friend" an adverse party. (NYCLA 743 at 2.) We agree with these conclusions; attorneys may not shift their conduct or assignments to non-attorneys in order to evade the Rules.

D. The Impact On Jury Service Of Attorney Use Of Social Media Websites For Research

Although the Committee concludes that attorneys may conduct jury research using social media websites as long as no "communication" occurs, the Committee notes the potential impact of jury research on potential jurors' perception of jury service. It is conceivable that even jurors who understand that many of their social networking posts and pages are public may be discouraged from jury service by the knowledge that attorneys and judges can and will conduct active research on them or learn of their online—albeit public—social lives. The policy considerations implicit in this possibility should inform our understanding of the applicable Rules.

In general, attorneys should only view information that potential jurors intend to be—and make—public. Viewing a public posting, for example, is similar to searching newspapers for letters or columns

written by potential jurors because in both cases the author intends the writing to be for public consumption. The potential juror is aware that her information and images are available for public consumption. The Committee notes that some potential jurors may be unsophisticated in terms of setting their privacy modes or other website functionality, or may otherwise misunderstand when information they post is publicly available. However, in the Committee's view, neither Rule 3.5 nor Rule 8.4(c) prohibit attorneys from viewing public information that a juror might be unaware is publicly available, except in the rare instance where it is clear that the juror intended the information to be private. Just as the attorney must monitor technological updates and understand websites that she uses for research, the Committee believes that jurors have a responsibility to take adequate precautions to protect any information they intend to be private.

E. Conducting On-Going Research During Trial

Rule 3.5 applies equally with respect to a jury venire and empanelled juries. Research permitted as to potential jurors is permitted as to sitting jurors. Although there is, in light of the discussion in Section III, infra, great benefit that can be derived from detecting instances when jurors are not following a court's instructions for behavior while empanelled, researching jurors mid-trial is not without risk. For instance, while an inadvertent communication with a venire member may result in an embarrassing revelation to a court and a disqualified panelist, a communication with a juror during trial can cause a mistrial. The Committee therefore re-emphasizes that it is the attorney's duty to understand the functionality of any social media service she chooses to utilize and to act with the utmost caution.

III. An Attorney Must Reveal Improper Juror Conduct to the Court

Rule 3.5(d) provides: "a lawyer shall reveal promptly to the court improper conduct by a member of the venire or a juror, or by another toward a member of the venire or a juror or a member of her family of which the lawyer has knowledge." Although the Committee concludes that an attorney may conduct jury research on social media websites as long as "communication" is avoided, if an attorney learns of juror misconduct through such research, she must promptly8 notify the court. Attorneys must use their best judgment and good faith in determining whether a juror has acted improperly; the attorney cannot consider whether the juror's improper conduct benefits the attorney.9

On this issue, the Committee notes that New York Pattern Jury Instructions ("PJI") now include suggested jury charges that expressly prohibit juror use of the internet to discuss or research the case. PJI 1:11 Discussion with Others - Independent Research states: "please do not discuss this case either among yourselves or with anyone else during the course of the trial. . . . It is important to remember that you may not use any internet service, such as Google, Facebook, Twitter or any others to individually or collectively research topics concerning the trial . . . For now, be careful to remember these rules whenever you use a computer or other personal electronic device during the time you are serving as juror but you are not in the courtroom." Moreover, PJI 1:10 states, in part, "in addition, please do not attempt to view the scene by using computer programs such as Goggle Earth. Viewing the scene either in person or through a computer program would be unfair to the parties . . . ." New York

criminal courts also instruct jurors that they may not converse among themselves or with anyone else upon any subject connected with the trial. NY Crim. Pro. §270.40 (McKinney's 2002).

The law requires jurors to comply with the judge's charge10 and courts are increasingly called upon to determine whether jurors' social media postings require a new trial. See, e.g.,Smead v. CL Financial Corp., No. 06CC11633, 2010 WL 6562541 (Cal. Super. Ct. Sept. 15, 2010) (holding that juror's posts regarding length of trial were not prejudicial and denying motion for new trial). However, determining whether a juror's conduct is misconduct may be difficult in the realm of social media. Although a post or tweet on the subject of the trial, even if unanswered, can be considered a "conversation," it may not always be obvious whether a particular post is "connected with" the trial. Moreover, a juror may be permitted to post a comment "about the fact [of] service on jury duty."11

IV. Post-Trial

In contrast to Rule 3.4(a)(4), Rule 3.5(a)(5) allows attorneys to communicate with a juror after discharge of the jury. After the jury is discharged, attorneys may contact jurors and communicate, including through social media, unless "(i) the communication is prohibited by law or court order; (ii) the juror has made known to the lawyer a desire not to communicate; (iii) the communication involves misrepresentation, coercion, duress or harassment; or (iv) the communication is an attempt to influence the juror's actions in future jury service." Rule 3.5(a)(5). For instance, NYSBA Opinion 246 found that "lawyers may communicate with jurors concerning the verdict and case." (NYSBA 246 (interpreting former EC 7-28; DR 7-108(D).) The Committee concludes that this rule should also permit communication via social media services after the jury is discharged, but the attorney must, of course, comply with all ethical obligations in any communication with a juror after the discharge of the jury. However, the Committee notes that "it [is] unethical for a lawyer to harass, entice, or induce or exert influence on a juror" to obtain information or her testimony to support a motion for a new trial. (ABA 319.)

V. Conclusion

The Committee concludes that an attorney may research potential or sitting jurors using social media services or websites, provided that a communication with the juror does not occur. "Communication," in this context, should be understood broadly, and includes not only sending a specific message, but also any notification to the person being researched that they have been the subject of an attorney's research efforts. Even if the attorney does not intend for or know that a communication will occur, the resulting inadvertent communication may still violate the Rule. In order to apply this rule to social media websites, attorneys must be mindful of the fact that a communication is the process of bringing an idea, information or knowledge to another's perception—including the fact that they have been researched.In the context of researching jurors using social media services, an attorney must understand and analyze the relevant technology, privacy settings and policies of each social media service used for jury research. The attorney must also avoid engaging in deception or misrepresentation in conducting such research, and may not use third parties to do that which the lawyer cannot. Finally, although attorneys may communicate with jurors after discharge of the jury in the circumstances

outlined in the Rules, the attorney must be sure to comply with all other ethical rules in making any such communication.

1. Rule 3.5(a)(4) states: "a lawyer shall not . . . (4) communicate or cause another to communicate with a member of the jury venire from which the jury will be selected for the trial of a case or, during the trial of a case, with any member of the jury unless authorized to do so by law or court order."

2. Missouri Rule of Professional Conduct 3.5 states: "A lawyer shall not: (a) seek to influence a judge, juror, prospective juror, or other official by means prohibited by law; (b) communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order."

3. The Committee also notes that the United States Attorney for the District of Maryland recently requested that a court prohibit attorneys for all parties in a criminal case from conducting juror research using social media, arguing that "if the parties were permitted to conduct additional research on the prospective jurors by using social media or any other outside sources prior to the in court voir dire, the Court's supervisory control over the jury selection process would, as a practical matter, be obliterated." (Aug. 30, 2011 letter from R. Rosenstein to Hon. Richard Bennet.) The Committee is unable to determine the court's ruling from the public file.

4. California Rule of Profession Conduct 2-100 states, in part: "(A) While representing a client, a member shall not communicate directly or indirectly about the subject of the representation with a party the member knows to be represented by another lawyer in the matter, unless the member has the consent of the other lawyer."

5. As of the date of this writing, May 2012, three of the most common social media services are Facebook, LinkedIn and Twitter.

6. Although the New York City Bar Association Formal Opinion 2010-2 ("NYCBA 2010-2") and SDCBA 2011-2 (both addressing social media "communication" in the context of the "No Contact" rule) were helpful precedent for the Committee's analysis, the Committee is unaware of any opinion setting forth a definition of "communicate" as that term is used in Rule 4.2 or any other ethics rule.

7. Rule 8.4 prohibits "conduct involving dishonesty, fraud, deceit or misrepresentation," and also states "a lawyer or law firm shall not: (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts or another." (Rule 8.4(c),(a).)

8. New York City Bar Association Formal Opinion 2012-1 defined "promptly" to mean "as soon as reasonably possible."

9. Although the Committee is not opining on the obligations of jurors (which is beyond the Committee's purview), the Committee does note that if a juror contacts an attorney, the attorney must promptly notify the court under Rule 3.5(d).

10. People v. Clarke, 168 A.D.2d 686 (2d Dep't 1990) (holding that jurors must comply with the jury charge).

11. US v. Fumo, 639 F. Supp. 2d 544, 555 (E.D. Pa. 2009) aff'd, 655 F.3d 288 (3d Cir. 2011) ("[The juror's] comments on Twitter, Facebook, and her personal web page were innocuous, providing no indication about the trial of which he was a part, much less her thoughts on that trial. Her statements about the fact of her service on jury duty were not prohibited. Moreover, as this Court noted, her Twitter and Facebook postings were nothing more than harmless ramblings having no prejudicial effect. They were so vague as to be virtually meaningless. [Juror] raised no specific facts dealing with the trial, and nothing in these comments indicated any disposition toward anyone involved in the suit.") (internal citations omitted).

NYCLA COMMITTEE ON PROFESSIONAL ETHICS

FORMAL OPINION

No.: 743

Date Issued: May 18, 2011

TOPIC: Lawyer investigation of juror internet and social networking postings during conduct of trial.

DIGEST:

It is proper and ethical under RPC 3.5 for a lawyer to undertake a pretrial search of a prospective juror's social networking site, provided that there is no contact or communication with the prospective juror and the lawyer does not seek to "friend" jurors, subscribe to their Twitter accounts, send tweets to jurors or otherwise contact them. During the evidentiary or deliberation phases of a trial, a lawyer may visit the publicly available Twitter, Facebook or other social networking site of a juror, but must not "friend," email, send tweets to jurors or otherwise communicate in any way with the juror, or act in any way by which the juror becomes aware of the monitoring. Moreover, the lawyer may not make any misrepresentations or engage in deceit, directly or indirectly, in reviewing juror social networking sites. In the event the lawyer learns of juror misconduct, including deliberations that violate the court's instructions, the lawyer may not unilaterally act upon such knowledge to benefit the lawyer's client, but must promptly comply with Rule 3.5(d) and bring such misconduct to the attention of the court before engaging in any further significant activity in the case.

RULES:

RPC 3.5, 4.1, 8.4

QUESTION:

After voir dire is completed and the trial commences, may a lawyer routinely conduct ongoing research on a juror on Twitter, Facebook and other social networking sites? If so, what are the lawyer's duties to the court under Rule of Professional Conduct 3.5?

OPINION:

This opinion considers lawyer investigations of jurors during an ongoing trial. With the advent of internet-based social networking services, additional complexities are introduced to the traditional rules barring contact between lawyers and jurors during trials.

New York RPC 3.5(a)(4) and (a)(5) provide that a lawyer shall not:

4. communicate or cause another to communicate with a member of the jury venire from which the jury will be selected for the trial of a case, or, during the trial of a case with any member of the jury unless authorized to do so by law or court order;

5. communicate with a juror or prospective juror after discharge of the jury if (i) the communication is prohibited by law or court order; (ii) the juror has made known to the lawyer a desire not to communicate; (iii) the communication involves misrepresentation, coercion, duress or harassment; or (iv) the communication is an attempt to influence the juror's actions in future jury service . . . .

Thus, the rules proscribe any direct or indirect communication with a juror or potential juror during trial, and prohibit certain categories of communication after the jury service is complete. It should also be noted that the RPC prevent a lawyer from doing indirectly, such as through a proxy, that which is directly proscribed for the lawyer. (RPC 8.4(a); 3.5).

A. Impermissible Communication

The RPC explicitly draw a distinction between conduct during trial, which is governed by RPC 3.5(a)(4), and conduct after discharge of the jury, which is regulated less strictly under RPC 3.5(a)(5). In fact, a lawyer's contact with jurors is divided, at least in practice, into three distinct areas. These are voir dire or jury selection, actual conduct of the trial, and post-verdict contact with jurors. As mentioned, any contact, direct or indirect, is proscribed as a matter of attorney ethics during the conduct of the trial, but permitted with certain conditions after discharge pursuant to RPC 3.5(a)(5).

Some authorities have examined a lawyer's use of internet resources to investigate potential jurors in the voir dire stage. For example, one recent Missouri decision considered and set aside a jury verdict in which a juror had specifically denied (falsely) any prior jury service. See Johnson v. McCullough, 306 S.W. 3d 551 (Mo. 2010). In holding that the juror had acted improperly, the Court observed that a more thorough investigation of the juror's background would have obviated the need to set aside the jury verdict and conduct a retrial. The trial court chided the attorney for failing to perform internet research on the juror, and granted a new trial, observing that a party should use reasonable efforts to examine the litigation history of potential jurors. 306 S.W. 3d at 559. A New Jersey appellate court similarly held that the plaintiff counsel's use of a laptop computer to google potential jurors was permissible and did not require judicial intervention for fairness concerns. See Carino v. Muenzen, No. A-5491-08T1, N.J. Super. Unpub. LEXIS 2154, at *26-27 (App. Div. Aug. 30, 2010); see also Jamila A. Johnson, "Voir Dire: to Google or Not to Google" (ABA Law Trends and News, GP/Solo & Small Firm Practice Area Newsletter, Fall 2008, Volume 5, No. 1).

In another context, the New York State Bar Association Committee on Professional Ethics, in Ethics Opinion 843, recently considered whether a lawyer could ethically access the publicly available social networking page of an unrepresented party or witness for use in litigation, including possible impeachment. The NYSBA concluded that the lawyer may ethically view and access the Facebook and MySpace profiles of a party other than the lawyer's client in litigation as long as the party's profile is available to all members in the network and the lawyer neither

"friends" the other party nor directs someone else to do so."[1] Drawing an analogy to jurors, we conclude that passive monitoring of jurors, such as viewing a publicly available blog or Facebook page, may be permissible.

During a trial, however, lawyers may not communicate with jurors outside the courtroom. Not only is direct or indirect juror contact during trial proscribed as a matter of attorney ethics, as a matter of law (which is outside the scope of this committee's jurisdiction), the courts proscribe any unauthorized contact between lawyers and sitting jurors.

Significant ethical concerns would be raised by sending a "friend request," attempting to connect via LinkedIn.com, signing up for an RSS feed for a juror's blog or "following" a juror's Twitter account. We believe that such contact would be impermissible communication with a juror.

Moreover, under some circumstances a juror may become aware of a lawyer's visit to the juror's website.[2] If a juror becomes aware of an attorney's efforts to see the juror's profiles on websites, the contact may well consist of an impermissible communication, as it might tend to influence the juror's conduct with respect to the trial.

B. Reporting Juror Misconduct

Lawyers who learn of impeachment or other useful material about an adverse party, assuming that they otherwise conform with the rules of the court, have no obligation to come forward affirmatively to inform the court of their findings. Such lawyers, absent other obligations under court rules or the RPC, may sit back confidently, waiting to spring their trap at trial.[3] On the other hand, a lawyer who learns of juror impropriety is bound by RPC 3.5 to promptly report such impropriety to the court. That rule provides that: "A lawyer shall reveal promptly to the court improper conduct by a member of the venire or a juror, or by another toward a member of the venire or a juror or a member of his or her family of which the lawyer has knowledge." RPC 3.5(d).

The standard jury charge in a civil or criminal case instructs jurors not to discuss the case with anyone outside the courtroom, not to conduct any independent investigation, not to view the scene of the incident through computer programs such as Google Earth, and not to perform any independent research on the internet. See PJI 1:10, 1:11. According to the New York pattern jury instruction:

---

[1] See NYSBA Ethics Op. 843, http://www.nysba.org/AM/Template.cfm?Section=Home&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=43208 at 2-3

[2] For example, as of this writing, Twitter apparently conveys a message to the account holder when a new person starts to "follow" the account, and the social networking site LinkedIn provides a function that allows a user to see who has recently viewed the user's profile. This opinion is intended to apply to whatever technologies now exist or may be developed that enable the account holder to learn the identity of a visitor.

[3] Lawyers should keep in mind that RPC 3.4 provides that a lawyer shall not "disregard or advise the client to disregard a standing rule of a tribunal. . .."

> It is important to remember that you may not use any internet services such as Google, Facebook, Twitter or any others to individually or collectively research topics concerning the trial, which includes the law, information about any of the issues in contention, the parties or the lawyers or the court.

Jurors have sometimes ignored instructions. For example, a New York juror googled defense counsel during trial, and discussed it at a social dinner.[4] A prominent television newscaster was criticized for tweeting on his Twitter account about his own jury service.[5] In a recent South Dakota case, a jury verdict was set aside after a juror performed his own internet research, which he shared with the other jurors.[6]

Any lawyer who learns of juror misconduct, such as substantial violations of the court's instructions, is ethically bound to report such misconduct to the court under RPC 3.5, and the lawyer would violate RPC 3.5 if he or she learned of such misconduct yet failed to notify the court. This is so even should the client notify the lawyer that she does not wish the lawyer to comply with the requirements of RPC 3.5. Of course, the lawyer has no ethical duty to routinely monitor the web posting or Twitter musings of jurors, but merely to promptly notify the court of any impropriety of which the lawyer becomes aware.

Further, the lawyer who learns of improper juror deliberations may not use this information to benefit the lawyer's client in settlement negotiations, or even to inform the lawyer's settlement negotiations. The lawyer may not research a juror's social networking site, ascertain the status of improper juror deliberations and then accept a settlement offer based on that information, prior to notifying the court. Rather, the lawyer must "promptly" notify the court of the impropriety—*i.e.*, before taking any further significant action on the case.

CONCLUSION:

It is proper and ethical under RPC 3.5 for a lawyer to undertake a pretrial search of a prospective juror's social networking site, provided that there is no contact or communication with the prospective juror and the lawyer does not seek to "friend" jurors, subscribe to their Twitter accounts, send jurors tweets or otherwise contact them. During the evidentiary or deliberation phases of a trial, a lawyer may visit the publicly available Twitter, Facebook or other social networking site of a juror but must not "friend" the juror, email, send tweets to the juror or otherwise communicate in any way with the juror or act in any way by which the juror becomes aware of the monitoring. Moreover, the lawyer may not make any misrepresentations or engage in deceit, directly or indirectly, in reviewing juror social networking sites. In the event the lawyer learns of juror misconduct, including deliberations that violate the court's instructions, the lawyer may not unilaterally act upon such knowledge to benefit the lawyer's client, but must promptly

---

[4] People vs. Jamison, 24 Misc. 3d 1238A, 243 N.Y.L.J. 42 (2006).

[5] Michael Hoenig, Juror Misconduct on the Internet, N.Y.L.J. October 8, 2009.

[6] Russo vs. Takata Corp., 2009 S.D. 83, 2009 S.D. Lexis 155 (Sept. 16, 2009).

comply with RPC 3.5(d) and bring such misconduct to the attention of the court, before engaging in any further significant activity in the case.

NEW YORK STATE BAR ASSOCIATION
Committee on Professional Ethics

OPINION 709 - 9/16/98 (55-97)

TOPIC: Use of Internet to advertise and to conduct law practice focusing on trademarks; use of Internet e-mail; use of trade names

DIGEST: Attorney may operate and advertise a trademark practice over the Internet, as long as attorney complies with (a) the Code's obligations to check client conflicts; (b) court rules requiring the posting of a statement of Client's Rights and Responsibilities; (c) the obligation to preserve client confidences by assuring that use of e-mail is reasonable; and (d) the Code's advertising rules and perhaps those of other jurisdictions. The attorney may not engage in or advertise a more limited form of trademark business under a trade name if the business constitutes the practice of law.

CODE: DR 1-102(A), DR 2-101, DR 2-101(B), DR 2-102, DR 2-102(B), DR 2-102(D), DR 2-101(F), DR 2-103(A), DR 2-106, DR 3-101(B), DR 4-101(A), DR 4-101(B), Canon 6, EC 2-10, EC 2-13, EC 3?5, EC 3-9, EC 4-1, EC 8-3

QUESTIONS

An attorney plans to create an Internet web site in connection with a business that will conduct trademark searches, render legal opinions on availability of trademarks, and file and prosecute applications to register trademarks. The web site will have the capability to take orders from clients from all over the country on the Internet, and charge their credit cards a pre-determined fee for each applicable service. The attorney will speak to clients by telephone when they request a legal opinion, but will otherwise rely on unencrypted Internet e?mail to communicate with clients.

We address the following questions in connection with this proposed conduct:

1. May an attorney make his or her services available through the Internet, including taking orders for conducting trademark searches, communicating with clients using Internet e-mail, conducting trademark searches, rendering legal opinions on trademark availability, filing trademark applications, and charging clients by credit card?

2. May an attorney advertise on the Internet utilizing a web site accessible throughout the United States where the attorney is licensed to practice law only in New York?

3. May an attorney licensed to practice only in New York render legal opinions to non-residents of New York, and if not, may the attorney limit his or her services to performing

trademark searches and filing trademark applications on behalf of clients who reside outside of New York, since such services may be performed by non-lawyers?

4. May the attorney operate his or her practice under a trade name as well as his or her own name (*e.g.*, advertising and operating under the trade name "The Trademark Store") and also state that The Trademark Store is operated by the "Law Offices of ____")? If the attorney only performs the trademark searching and filing services that may be performed by non-lawyers, and does not render legal opinions, may the attorney operate the business under a trade name without using his or her own name?

1. Legal Practice on the Internet

There is no express provision in the Lawyer's Code of Professional Responsibility (the "Code") that addresses practicing law over the Internet. The Committee believes that using the Internet to take orders for trademark searches, conduct trademark searches, render legal opinions and file trademark applications is analogous to conducting a law practice by telephone or facsimile machine and is likewise permissible, subject to the same restrictions applicable to communication by those means. Some issues peculiar to practice on the Internet warrant additional comment, however.

A. Statement of Client's Rights and Responsibilities

New York's court rules require the posting of a Statement of Client's Rights and Responsibilities in a lawyer's office, and apply by their terms to any attorney who has an office in the state. 22 N.Y.C.R.R. § 1210.1. As a result, such rules may apply even where the attorney-client relationship is conducted exclusively through the Internet and the lawyer does not typically meet clients in the lawyer's office. In such circumstances it would be prudent for the attorney to achieve substantial compliance with the terms of the rule (requiring posting of the Statement in the office "in a manner visible to clients") by including the full text of the Statement on the attorney's web site.

B. Conflicts Checks

Next, DR 5-105(E) provides that New York lawyers must maintain a system of keeping records of prior engagements and checking them before undertaking a new matter to assure that the attorney will not violate DR 5-105's and DR 5-108's prohibitions on conflicting engagements. Practicing law for clients by means of the Internet does not give rise to any exemption from this fundamental obligation to avoid conflicts and not to undertake a new representation without checking to assure that it does not create an impermissible conflict. *See generally* N.Y. State 664 (1994) (requiring conflicts check by lawyer providing specific legal advice to clients by means of "900" telephone service). We recognize, however, that a conflicts check is not required where the attorney's interaction is limited to providing general information of an educational nature, no confidential information is obtained from a client and no specific advice tailored to a client's particular circumstances is rendered. *Id.; cf.* N.Y. 625 (1992); N.Y. State 636 (1992). In such circumstances, the recipient of such general advice need not be included in the lawyer's records of past engagements.

C. Reliability of Internet Information

To the extent that the attorney in performing legal research for clients relies on information obtained from searching of Internet sites, the attorney's duty under Canon 6 to represent the client competently requires that the attorney take care to assure that the information obtained is reliable.

D. Use of Internet E-Mail

As to the attorney's use of Internet e-mail to communicate with clients, we note that the fiduciary relationship between an attorney and client requires the preservation of confidences and

secrets, EC 4-1, and an attorney is prohibited from "knowingly" revealing a client confidence or secret. DR 4-101(B). Significantly, the Code expressly requires attorneys to "exercise reasonable care" to prevent others at his or her firm from disclosing a client's confidences or secrets, DR 4-101(D), and EC 4-4 provides that a "lawyer should endeavor to act in a manner which preserves the evidentiary privilege; for example, the lawyer should avoid professional discussions in the presence of persons to whom the privilege does not extend." It is fair to state that an attorney has a duty to use reasonable care to protect client confidences and secrets; whether the use of Internet e-mail is consistent with that duty depends upon the likelihood of interception.

Other ethics committees that have considered this or analogous issues have reached inconsistent conclusions. *Compare* Az. Op. 97-04 (e-mail may pose a risk to confidentiality); Iowa Op. 96-1 (attorneys must obtain waiver from clients as to e-mail security risk); N.Y. City 94-11 (advising that an attorney should use caution and consider security measures when speaking to a client via cordless or cellular telephone because of the risk that the client's confidences or secrets may be overheard); *with* D.C. Op. 281 (1998) (no *per se* rule barring use of unencrypted internet e-mail to transmit client confidences); South Carolina Op. 97-08 (examining the privacy of Internet communications in view of current technology and laws prohibiting interception or monitoring of e-mail communications, and concluding that Internet users may have a reasonable expectation of confidentiality); Vt. Op. 97-5 (e-mail may pose no risk to confidentiality).

The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510 *et seq.*, criminalizes the interception of e-mail transmissions and also appears to mitigate the risk of loss of the evidentiary privilege. 18 U.S.C. § 2517(4) ("[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of [the ECPA] shall lose its privileged character"). Similarly, in 1998 New York enacted comparable protection for the evidentiary privilege in an amendment to the CPLR.[1] Although the federal and New York statutes may resolve the question of whether use of Internet e-mail waives the evidentiary privilege (a question of law outside the scope of this Committee's jurisdiction), at least to the extent the privilege at issue is governed by federal or New York law, the statutes do not directly resolve the lawyer's independent ethical duty to avoid disclosure of a client's confidences and secrets. The lawyer's ethical duty is broader than the obligation to preserve the privilege, as the Code extends the duty of non-disclosure to client "secrets," which are explicitly defined by the Code to encompass certain client-related information that is *not* protected by the evidentiary attorney-client privilege. DR 4-101(A), (B). Consequently, the recent additions in federal and state law providing that use of e-mail does not by itself jeopardize the applicability of the attorney-client privilege cannot dispose of the ethical issue.

In considering the ethical issue, we believe that the criminalization of unauthorized interception of e-mail certainly enhances the reasonableness of an expectation that e-mails will be as private as other forms of telecommunication. That prohibition, together with the developing experience from the increasingly widespread use of Internet e-mail, persuades us that concerns over lack of privacy in the use of Internet e-mail are not currently well founded. So far as we are aware, there is little evidence that the use of unencrypted Internet e-mails has resulted in a greater risk of unauthorized disclosure than is posed by other forms of communication that are commonly used without compromising ethical obligations, such as telephones and facsimile machines. We therefore conclude that lawyers may in ordinary circumstances utilize unencrypted Internet e-mail to transmit confidential information without breaching their duties of confidentiality under Canon 4 to their clients, as the technology is in use today. Despite this general conclusion, lawyers must always act reasonably in choosing to use e-mail for confidential communications, as with any other means of communication. Thus, in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential

information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail.

A lawyer who uses Internet e-mail must also stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost.[2] It is also sensible for lawyers to discuss with clients the risks inherent in the use of Internet e-mail, and lawyers should abide by the clients' wishes as to its use.

E. Payment By Credit Card

There is nothing in the Code prohibiting an attorney from accepting payment by credit card as long as the fee charged is not excessive and the fee arrangement does not otherwise violate any Code provision. N.Y. State 399 (1975); N.Y. State 362 (1974); *see* DR 2-106. The lawyer's duty to safeguard client interests and property also requires the lawyer who accepts payment by credit card via the Internet to assure that the privacy of the client's credit card information will be preserved.

2. Advertising on the Internet

The Code's advertising rules are intended to protect the public from false and misleading advertisements. There is no ethical distinction to be drawn among different forms of advertising directed to a general population. *See, e.g., Shapero v. Kentucky Bar Assoc.*, 486 U.S. 466, 473 (1988) ("lawyer advertising cases have never distinguished among various modes of written advertising to the general public")*; In re Koffler*, 432 N.Y.S.2d 872, 875 (Ct. App. 1980) (direct mail solicitation by attorneys of potential clients is constitutionally protected commercial speech), *cert. denied*, 450 U.S. 1026 (1981); *cf* ABA Model Rule 7.2(a) (permitting advertising in "public media," including " a telephone directory, legal directory, newspaper or other periodical, outdoor advertising, radio or television, or through written or recorded communication"). Accordingly, we believe that advertising via the Internet — an electronic form of public media — is permissible as long as the advertising is not false, deceptive or misleading, and otherwise adheres to the requirements set forth in the Code. DR 2-101, DR 2-102, EC 2-10.

In addition to the other guidelines for lawyer advertising set forth in DR 2-101, we note that DR 2-101(F) requires retention and in some circumstances filing of advertisements with a departmental disciplinary committee, depending upon the medium used to distribute the advertisement. Thus, broadcasts must be tape recorded and preserved by the lawyer for one year; a copy of mailed advertisements must be filed as noted, and the address list retained by the attorney for a year. We conclude that an Internet web site advertisement is more analogous to a radio or TV broadcast, in which the attorney has no means of identifying the audience, than it is to a mass mailing in which the address list is within the attorney's control. Therefore, the attorney must keep a copy of any Internet advertisement for a period of not less than one year following its last use, but need not file a copy with a departmental disciplinary committee. The copy may be maintained by the attorney in electronic form.

There is no ethical prohibition in the Code against advertising to solicit clients who reside outside the state of New York with respect to matters as to which the lawyer may competently and lawfully practice. However, any Internet advertisement should inform a potential client of the jurisdiction in which the attorney is licensed, and should not mislead the potential client into believing that the attorney is licensed in a jurisdiction where the attorney is not licensed. *See* DR

2-102(D); ABA/BNA Lawyers Manual on Professional Conduct 81:551 at 57 ("lawyer's Web page should clearly identify those states in which he is licensed to practice"); South Carolina Op. 94-27 (1995) (any advertisement by a lawyer on the Internet that may reach potential clients in jurisdictions where lawyer is not admitted to practice must clearly identify the geographic limitations of lawyer's practice or risk being deemed misleading); *see also Florida Bar v. Kaiser*, 397 So.2d 1132, 1133 (Fl. Sup. Ct. 1981) (lawyer engaged in unauthorized practice where his law firm's advertisements gave the impression that he was authorized to practice in Florida). [3]

3. Services to Clients Outside New York

DR 3-101(B) provides that a lawyer "shall not practice law in a jurisdiction where to do so would be in violation of regulations of the profession in that jurisdiction." Thus, whether a lawyer licensed only in New York may render legal opinions over the Internet to clients who reside outside of New York depends on whether the attorney's conduct constitutes the unauthorized practice of law in the other jurisdiction. That question is beyond the scope of this Committee's jurisdiction, though we note that lawyers licensed in one state may appropriately render legal services to clients resident elsewhere in many circumstances. N.Y. State 375 (1975). *But see Birbrower, Montalbano, Condon & Frank v. Superior Court of Santa Clara County*, 70 Cal. Rptr. 2d 304, 306 (Cal. Sup. Ct. 1998) (New York firm that performed legal services in California engaged in the unauthorized practice of law in violation of California statute). We are similarly unable to opine on whether the limitation of the practice to federal trademark issues affects the applicability of state laws regarding unauthorized practice. *See* Charles W. Wolfram, "Sneaking Around in the Legal Profession: Interjurisdictional Unauthorized Practice by Transactional Lawyers," 36 S. Tex. L.J. 665 (1995).

Finally, if an attorney licensed only in New York limits his or her services to trademark searches and filing trademark applications as non-lawyers are typically permitted to do, whether or not the attorney may provide such limited services to clients who reside outside of New York in matters arising in a non-New York jurisdiction is governed by the laws and rules of the other jurisdiction, and therefore is also beyond the scope of this Committee.

4. Use of a Trade Name for a Law Practice

Operating the proposed law practice under a trade name is prohibited by the Code. DR 2-102(B) provides that "[a] lawyer in private practice shall not practice under a trade name." *See In re von Wiegen*, 481 N.Y.S. 2d 40 (Ct. App. 1984) (use of phrase "The Country Lawyer" immediately below lawyer's name is acceptable; *In re Shephard*, 459 N.Y.S.2d 632, 633 (3rd Dep't 1983) (finding "The People's Law Firm" was a prohibited trade name); *In re Shapiro*, 455 N.Y.S. 2d 604, 605 (1st Dep't 1982) (finding "People's Legal Clinic, Inc." was a prohibited trade name). Operating the proposed law practice under a trade name, while simultaneously indicating in advertising materials that the company is operated by the attorney's law office, is likely to be confusing and misleading to the public as to whether the company and law office are separate entities.

Given the prohibition against attorneys practicing under a trade name in DR 2?102(B), whether an attorney may operate under a trade name a business limited to providing services that can permissibly be offered by non-lawyers depends on whether the attorney's conduct constitutes the practice of law. Although certain activities may be performed by lawyers and non-lawyers alike, this Committee has previously opined that certain activities that may be performed by non-lawyers constitute the practice of law when done by attorneys. *See, e.g.*, N.Y. State 705 (1998) (handling real estate tax reduction proceedings); N.Y. State 678 (1996) (providing divorce mediation services); N.Y. State 557 (1984) (providing accountant services).

On the other hand, this Committee also has opined that an attorney may maintain a separate business that does not involve the practice of law, and operate that business under a trade name, provided that the attorney does not use the separate business as a means of soliciting legal work in violation of any statute or court rule, does not recommend that clients of the law practice purchase a product of the separate business, does not hold himself or herself out as an attorney in connection with the separate business, and does not otherwise violate any ethical or legal rules. N.Y. State 636 (1992) (finding no *per se* ethical proscription to law firm establishing separate business selling will forms operating under the trade name "The Will Store" provided that the phrase was not used in conjunction with the names of the attorney principals, the business did not constitute the practice of law, and the separate business is not used to solicit legal practice); *cf.* N.Y. State 662 (1994) (refraining from holding oneself out as a lawyer may satisfy the literal language of N.Y. State 557, but would constitute deception in violation of DR 1?102(A)(4) where lawyer refrains in order to avoid an ethical prohibition and solicit legal work); EC 2?13 ("to avoid the possibility of misleading persons with whom a lawyer deals, a lawyer should be scrupulous in the representation of professional status").

The lawyer must closely scrutinize the services provided to make certain that the services do not involve the exercise of an attorney's professional judgment, which would constitute the practice of law. We provided the following guidance in N.Y. State 636:

[T]o the extent that the wills are individualized and offered as a specific solution to individual problems or other services requiring the professional judgment of a lawyer are rendered, the business becomes the practice of law. EC 3-5. Furthermore, if in selling such forms to individual members of the public, an employee provides assistance or advice in selecting the appropriate form or forms or in adapting their language to particular circumstances, the business becomes the practice of law.

Therefore, even though trademark searches and application filings may be performed by non-lawyers, to the extent that the attorney invokes his or her professional legal judgment in conducting searches or filing applications, the business becomes the practice of law and practicing under a trade name is prohibited.

CONCLUSION

The questions are answered in accordance with this Opinion.

---

[1] New CPLR § 4547 provides:

No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.

[2] We note that recent press reports concerning a lack of security arising from the use of Internet e-mail have not reflected interceptions of the content of e-mails, but instead the possible effect of the use of e-mail programs on the security of the contents of the files stored in a computer that is connected to the Internet. *See, e.g.,* Denise Caruso, "Technology: As long as software code is kept secret, Internet security is at risk," N.Y. Times, Aug. 17, 1998, at D3. The security risk at issue is wholly separate from the use of e-mail to transmit confidential communications, as the content of e-mails is not itself intercepted, and the possible interception of the contents of stored computer files potentially occurs when a person receives an e-mail from the would-be interceptor. Should it become clear that a lawyer's use of Internet e-mail exposes the contents of the lawyer's

computer files to a meaningful risk of unauthorized interception, lawyers will, of course, be unable to use Internet e-mail without taking steps to eliminate such risk.

[3] We express no view as to whether Internet advertising may also be subject to the rules regulating lawyer advertising of other jurisdictions in which the advertising appears and from which potential clients are solicited. Other states have opined that lawyers may advertise over the Internet as long as they comply with that state's ethics and rules on advertising but have not necessarily asserted that such state's rules apply to lawyers licensed and practicing outside that state. Utah Op. 97-10 (attorney may advertise service on web page provided that attorney complies with the state's advertising rules); Iowa Op. 96-1 (Iowa lawyers advertising on the Web page must comply with state's ethics rules including publication of mandatory disclosures), Penn. Op. 96-17 (law firm web site is permitted subject to state's advertising ethics rules, including disclosures of the geographic location of the law office and recordkeeping requirements); Tenn. Op. 95-A-57 (Tennessee lawyer posting firm brochure on World Wide Web must comply with ethical rules regarding publicity); Tex. Disc. Rules of Prof. Conduct, Part 7, Comment 17 (lawyers' Web sites are public media advertisement subject to state advertising rules);*see also* David Bell, *Internet Use Raises Ethics Questions*, Cal. St. B. J. at 36-37 (April 1996) (California rule and statute on attorney advertising applies to attorneys advertising on Internet); *Ethics Update*, Florida Bar News, Jan. 1, 1996 (lawyers' computer ads and industry web site on home pages are subject to Florida ethics rules on advertisements disseminated in electronic media). In addition, at least one state opinion suggests that lawyers should publish separate, unconnected web sites for in-state and out-of-state offices of the same law firm. Iowa Op. 96-14.

NYCLA COMMITTEE ON PROFESSIONAL ETHICS

OPINION No. 738

Date Issued: 3/24/08

Topic

Searching inadvertently sent metadata in opposing counsel's electronic documents.

Digest

A lawyer who receives from an adversary electronic documents that appear to contain inadvertently produced metadata is ethically obligated to avoid searching the metadata in those documents. This opinion does not address electronic documents in the form of document discovery. While attorneys are advised to take due care in sending correspondence, contracts, or other documents electronically to opposing counsel by scrubbing the documents to ensure that they are free of metadata, such as tracked changes and other document property information, an adversary may not ethically take advantage of a breach in the attorney's care by intentionally searching for this metadata. Using the metadata is unethical if the recipient's intent is to investigate opposing counsel's work product or client confidences or secrets or if the recipient is likely to find opposing counsel's work product or client confidences or secrets by searching the metadata. Using the metadata is appropriate in circumstances where the adversary has intentionally sent it, such as where the lawyers are using tracked changes to show one another their changes to a document. Without such a prior course of conduct to the contrary, however, there is a presumption that disclosure of metadata is inadvertent and would be unethical to view.

Code Provisions

DR 1-102(A)(4), DR 1-102(A)(5), DR 4-101; EC 4-1; EC 7-1, DR 7-101, DR 7-102(A)(8)

Question

Is an attorney ethically permitted to search metadata[1] in electronic documents sent by opposing counsel, which is not in the form of a document production?

Opinion

A lawyer who sends opposing counsel correspondence, contracts, or other similar documents electronically – as is now often the case – has the burden to take due care in appropriately scrubbing documents prior to sending them outside of the office or in sending them

[1] Metadata means information describing the history, tracking, or management of an electronic document, which may include changes that were made to a document and other document properties. *See* Advisory Committee note to Federal Rule of Civil Procedure 26(f) (Dec. 2006).

in a way that otherwise ensures that the documents are free of metadata.[2] As the ethics committees of several state bar associations and the American Bar Association ("ABA") have recently opined on the issue of searching metadata in documents and have come to differing conclusions, the NYCLA Ethics Committee has determined that it would be of interest also to consider this issue. This opinion provides guidance under the Code for the lawyer who receives from opposing counsel electronic correspondence, contracts, or other similar documents – not in the form of document discovery – that contain metadata.[3]

While the New York Code of Professional Responsibility (the "Code") does not directly address this issue, several disciplinary rules and ethical considerations in the Code relate to the topic. A lawyer is prohibited from engaging in conduct that involves "dishonesty, fraud, deceit, or misrepresentation" or is "prejudicial to the administration of justice." DR 1-102(A)(4); DR 1-102(A)(5). Yet, a lawyer is ethically obligated to represent clients zealously, to assist in achieving their legitimate goals, and to preserve their confidences and secrets. *See* DR 7-101 ("Representing a Client Zealously"); DR 4-101 ("Preservation of Confidences and Secrets of a Client"); EC 4-1. EC 7-1 cautions that a lawyer should represent the client "zealously within the bounds of the law, which includes Disciplinary Rules and enforceable professional regulations." Further, DR 7-102(A)(8) prohibits a lawyer from knowingly engaging in conduct "contrary to a Disciplinary Rule." As is often the case, the ethics issues implicated here involve balancing the duty of zealous representation with the lawyer's duty of being an officer of the court.

Similar to Inadvertent Disclosure

In a 2002 opinion, the NYCLA Ethics Committee advised on whether a lawyer has ethical obligations when receiving inadvertently disclosed privileged information. NYCLA Op. 730 (2002). The Committee determined that the Code does not directly address the issue, but that Model Rule of Professional Conduct 4.4(b) adopted by the ABA – "A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender" – provided guidance that New York lawyers should emulate. *Id.* Thus, the Committee instructed an attorney who received an inadvertent disclosure with privileged information to report the disclosure to opposing counsel without further review of the document. *Id.*; *see also* New York City Bar Op. 2003-04 (2003) (opining that in the case of inadvertent disclosure, the receiving attorney must notify the sending attorney of the disclosure).

---

[2] Scrubbing means removing metadata such as tracked changes and comments from a document. A document may be scrubbed using commercially available software, but this software is not always successful in removing all metadata. Other forms of electronically sending material in a protected manner include sending the document as a PDF after scanning it. *See* Roy Simon, Simon's New York Code of Professional Responsibility Annotated, at 589 (2007 ed.) ("[I]t is more and more difficult for lawyers to justify ignorance about metadata or to justify sending sensitive metadata to another lawyer, and more and more likely that 'reasonable care' includes removing metadata before sending a document.").

[3] This opinion does not address electronic documents that have been produced in the way of discovery, which often includes metadata that by agreement may be viewed by attorneys in the course of litigation. For recent discussions in other jurisdictions of ethics in reviewing metadata in the context of electronic document discovery, see Maryland State Bar Opinion 2007-09 (2007) and District of Columbia Ethics Opinion 341 § B (2007).

By actively mining an adversary's correspondence or documents for metadata under the guise of zealous representation, a lawyer could be searching only for attorney work product or client confidences or secrets that opposing counsel did not intend to be viewed. An adversary does not have the duty of preserving the confidences and secrets of the opposing side under DR 4-101 and EC 4-1. Yet, by searching for privileged information, a lawyer crosses the lines drawn by DR 1-102(A)(4) and DR 1-102(A)(5) by acting in a manner that is deceitful and prejudicial to the administration of justice. Further, the lawyer who searches an adversary's correspondence for metadata is intentionally attempting to discover an inadvertent disclosure by the opposing counsel, which the Committee has previously opined must be reported to opposing counsel without further review in certain circumstances. *See* NYCLA Op. 730 (2002). Thus, a lawyer who seeks to discover inadvertent disclosures of attorney work product or client confidences or secrets or is likely to find such privileged material violates DR 1-102(A)(4) and DR 1-102(A)(5).

Other situations may arise where it is not clear whether supplying a document containing metadata is an "inadvertent" disclosure. For example, if a lawyer sends material clearly showing tracked changes, the recipient will have to determine from the circumstances in that matter whether the sender intended to send a document showing changes or whether it appeared to be a mistake and the document is likely to contain privileged material. If the receiving lawyer reasonably believes that the disclosure was intentional because, for example, they had been using tracked changes to show one another the changes that each was making, it is not unethical for the receiving lawyer to review the metadata. Without such a prior understanding or course of conduct to the contrary, however, there is a presumption that disclosure of metadata is inadvertent and would be unethical to view.

Also, a situation may arise where a lawyer has a reason for investigating metadata that is not for the purpose of intending to uncover attorney work product or client confidences or secrets or if the lawyer is likely to find such privileged material. For example, if a lawyer is facing a *pro se* litigant and suspects that a lawyer is nonetheless drafting the pleadings for the *pro se* litigant, the lawyer who searches the properties to see whether a lawyer has drafted the material is not likely to uncover attorney work product or client confidences or secrets and may not be intending to uncover such material because a *pro se* litigant does not have the attorney work product protection. And, as mentioned above, this opinion does not consider electronic documents in the form of document discovery.

ABA and NYSBA Difference of Opinions

The ABA Ethics Committee issued an opinion in 2006 that permitted review of metadata in documents opposing counsel sends electronically. *See* ABA Formal Op. 06-442 (2006). The ABA explained that its ethics committee disagrees with authorities that have related the issue of metadata in an adversary's electronic documents to a lawyer's honesty. *Id.* (disagreeing with New York State Bar Association ("NYSBA") Ethics Opinion 749 (2001), *aff'd by* NYSBA Op. 782 (2004), that did not permit mining for such metadata).[4] Further, the ABA explained that

[4] The ABA also disagreed with a Florida Bar Professional Ethics Committee proposed opinion, which has since been adopted, that was similar to the NYSBA opinion. *See* Prof'l Ethics of the Florida Bar Op. 06-2

Model Rule of Professional Conduct 4.4(b), which relates to a lawyer's receipt of inadvertently sent information, is the "most closely applicable rule" but determined that the issue is not sufficiently related. *Id.* at 3 & n.7 ("The Committee does not characterize the transmittal of metadata either as inadvertent or as advertent, but observes that the subject may be fact specific."). Instead, the ABA focused on the duties of the attorney sending the electronic data to scrub the data properly to avoid disclosing client confidences and secrets. *See id.*

As noted above, the NYSBA Ethics Committee advised that a lawyer may not use available technology to "surreptitiously examine" electronic documents. NYSBA Op. 749 (2001). The NYSBA found that by mining for metadata, a lawyer would "violate the letter and spirit" of the disciplinary rules that promote "the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship." *Id.* (citing DR 1-102(A)(4), (5); DR 4-101; DR 7-102(A)(8)).[5]

While this Committee agrees that every attorney has the obligation to prevent disclosing client confidences and secrets by properly scrubbing or otherwise protecting electronic data sent to opposing counsel, mistakes occur and an attorney may neglect on occasion to scrub or properly send an electronic document. The question here is whether opposing counsel is permitted to take advantage of the sending attorney's mistake and hunt for the metadata that was improperly left in the document.

This Committee finds that the NYSBA rule is a better interpretation of the Code's disciplinary rules and ethical considerations and New York precedents than the ABA's opinion on this issue. Thus, this Committee concludes that when a lawyer sends opposing counsel correspondence or other material with metadata, the receiving attorney may not ethically search the metadata in those electronic documents with the intent to find privileged material or if finding privileged material is likely to occur from the search.

Conclusion

(2006). Since the ABA opinion came out, the Alabama and Arizona state bar associations have also issued ethics opinions that prohibit mining an adversary's inadvertent electronic metadata. *See* Alabama State Bar Op. 2007-02 (2007); State Bar of Arizona Ethics Op. 07-03 (2007). The District of Columbia has recently issued an ethics opinion that prohibits a lawyer from mining an adversary's electronic metadata only where the lawyer has actual knowledge that the metadata was inadvertently sent. D.C. Ethics Op. 341 § A (2007).

[5] While New York does not follow the ABA Model Rules and thus is not bound by an ABA ethics opinion, the conflicting opinions still may affect New York lawyers. *See* Roy Simon, Simon's New York Code of Professional Responsibility Annotated, at 589 (2007 ed.):

> Given that lawyers in most jurisdictions in the United States have adopted the ABA Model Rules, a [New York] lawyer sending a digital attachment to an out-of-state lawyer should assume that the receiving lawyer may ethically study the metadata embedded in the document as long as the lawyer notifies the sending lawyer that the metadata has been received. Indeed, if a receiving lawyer believes that the metadata was sent deliberately rather than inadvertently – often a plausible conclusion, given the ease of removing metadata – then the lawyer need not even notify the sender that the metadata has been received and even in New York may freely exploit it.

A lawyer who receives from an adversary electronic documents that appear to contain inadvertently produced metadata is ethically obligated to avoid searching the metadata in those documents. While attorneys are advised to take due care in sending correspondence, contracts, or other documents to opposing counsel by scrubbing the documents to ensure that they are free of metadata, an adversary may not ethically take advantage of a breach in the attorney's care by intentionally searching for metadata. Using the metadata is unethical if the recipient's intent is to investigate opposing counsel's work product or client confidences or secrets or if the recipient is likely to find opposing counsel's work product or client confidences or secrets by searching the metadata. Without a prior understanding to the contrary, there is a presumption that disclosure of metadata is inadvertent and would be unethical to view.

New York State Bar Association
Committee on Professional Ethics

Opinion 1019 (8/6/2014)

Topic: Confidentiality; Remote Access to Firm's Electronic Files

Digest: A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Rules: 1.0(j), 1.5(a), 1.6, 1.6(a), 1.6(b), 1.6(c), 1.15(d).

QUESTION

1. May a law firm provide its lawyers with remote access to its electronic files, so that they may work from home?

OPINION

2. Our committee has often been asked about the application of New York's ethical rules -- now the Rules of Professional Conduct -- to the use of modern technology. While some of our technology opinions involve the application of the advertising rules to advertising using electronic means, many involve other ethical issues. See, *e.g.:*

N.Y. State 680 (1996). Retaining records by electronic imaging during the period required by DR 9-102(D) [now Rule 1.15(d)].

N.Y. State 709 (1998). Operating a trademark law practice over the internet and using e-mail.

N.Y. State 782 (2004). Use of electronic documents that may contain "metadata".

N.Y. State 820 (2008). Use of an e-mail service provider that conducts computer scans of emails to generate computer advertising.

N.Y. State 833 (2009). Whether a lawyer must respond to unsolicited emails requesting representation.

N.Y. State 842 (2010). Use of a "cloud" data storage system to store and back up client confidential information.

N.Y. State 940 (2012). Storage of confidential information on off-site backup tapes.

N.Y. State 950 (2012). Storage of emails in electronic rather than paper form.

3. Much of our advice in these opinions turns on whether the use of technology would violate the lawyer's duty to preserve the confidential information of the client. Rule 1.6(a) sets forth a simple prohibition against disclosure of such information, i.e. "A lawyer shall not knowingly reveal confidential information, as defined in this Rule . . . unless . . . the client gives informed consent, as defined in Rule 1.0(j)." In addition, Rule 1.6(c) provides that a lawyer must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except as provided in Rule 1.6(b).

4. Comment 17 to Rule 1.6 provides some additional guidance that reflects the advent of the information age:

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered to determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

5. As is clear from Comment 17, the key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure and that the lawyer has taken reasonable precautions in the use of the technology.

6. In some of our early opinions, despite language indicating that the inquiring lawyer must make the reasonableness determination, this Committee had reached general conclusions. In N.Y. State 709, we concluded that there is a reasonable expectation that e-mails will be as private as other forms of telecommunication, such as telephone or fax machine, and that a lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information, unless there is a heightened risk of interception. We also noted, however, that "when the confidential information is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted internet e-mail." Moreover, we said the lawyer was obligated to stay abreast of evolving technology to assess changes in the likelihood of interception, as well as the availability of improved technologies that might reduce the risks at a reasonable cost.

7. In N.Y. State 820, we approved the use of an internet service provider that scanned e-mails to assist in providing user-targeted advertising, in part based on the published privacy policies of the provider.

8. Our more recent opinions, however, put the determination of reasonableness squarely on the inquiring lawyer. See, e.g. N.Y. State 842, 940, 950. For example, in N.Y. State 842, involving

the use of "cloud" data storage, we were told that the storage system was password protected and that data stored in the system was encrypted. We concluded that the lawyer could use such a system, but only if the lawyer took reasonable care to ensure that the system was secure and that client confidentiality would be maintained. We said that "reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

(1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

(2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

(3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

(4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

Moreover, in view of rapid changes in technology and the security of stored data, we suggested that the lawyer should periodically reconfirm that the provider's security measures remained effective in light of advances in technology. We also warned that, if the lawyer learned information suggesting that the security measures used by the online data storage provider were insufficient to adequately protect the confidentiality of client information, or if the lawyer learned of any breaches of confidentiality by the provider, then the lawyer must discontinue use of the service unless the lawyer received assurances that security issues had been sufficiently remediated.

9. Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system. See, e.g. Matthew Goldstein, "Law Firms Are Pressed on Security For Data," N.Y. Times (Mar. 22, 2014) at B1 (corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount; companies are asking law firms to stop putting files on portable thumb drives, emailing them to non-secure iPads or working on computers linked to a shared network in countries like China or Russia where hacking is prevalent); Joe Dysart, "Moving Targets: New Hacker Technology Threatens Lawyers' Mobile Devices," ABA Journal 25 (September 2012); Rachel M. Zahorsky, "Being Insecure: Firms are at Risk Inside and Out," ABA Journal 32 (June 2013); Sharon D. Nelson, John W. Simek & David G. Ries, Locked Down: Information Security for Lawyers (ABA Section of Law Practice Management, 2012).

10. In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected. Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information. However, assuming that the law firm determines that its precautions are reasonable, we believe it may provide such remote access. When the law firm is able to make a determination of reasonableness, we do not believe that client consent is necessary.

11. Where a law firm cannot conclude that its precautions would provide reasonable protection to client confidential information, Rule 1.6(a) allows the law firm to request the client's informed consent. See also Comment 17 to Rule 1.6, which provides that a client may give informed consent (as in an engagement letter or similar document) to the use of means that would otherwise be prohibited by the rule. In N.Y. State 842, however, we stated that the obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must take reasonable care to affirmatively protect a client's confidential information. Consequently, we believe that before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision.

CONCLUSION

12. A law firm may use a system that allows its lawyers to access the firm's document system remotely, as long as it takes reasonable steps to ensure that confidentiality of information is maintained. Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients. If the firm cannot conclude that its security precautions are reasonable, then it may request the informed consent of the client to its security precautions, as long as the firmdiscloses the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j).

New York State Bar Association
Committee on Professional Ethics

Opinion 1020 (9/12/2014)

Topic: Confidentiality; use of cloud storage for purposes of a transaction

Digest: Whether a lawyer to a party in a transaction may post and share documents using a "cloud" data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

Rules: 1.1, 1.6

FACTS

1. The inquirer is engaged in a real estate practice and is looking into the viability of using an electronic project management tool to help with closings. The technology would allow sellers' attorneys, buyers' attorneys, real estate brokers and mortgage brokers to post and view documents, such as drafts, signed contracts and building financials, all in one central place.

QUESTION

2. May a lawyer representing a party to a transaction use a cloud-based technology so as to post documents and share them with others involved in the transaction?

OPINION

3. The materials that the inquirer seeks to post, such as drafts, contracts and building financials, may well include confidential information of the inquirer's clients, and for purposes of this opinion we assume that they do.[1] Thus the answer to this inquiry hinges on whether use of the contemplated technology would violate the inquirer's ethical duty to preserve a client's confidential information.

4. Rule 1.6(a) contains a straightforward prohibition against the knowing disclosure of confidential information, subject to certain exceptions including a client's informed consent, and Rule 1.6(c) contains the accompanying general requirement that a lawyer "exercise reasonable care to prevent … [persons] whose services are utilized by the lawyer from disclosing or using confidential information of a client."

5. Comment [17] to Rule 1.6 addresses issues raised by a lawyer's use of technology:

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in

determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

6. In the recent past, our Committee has repeatedly been asked to provide guidance on the interplay of technology and confidentiality. N.Y. State 1019 (2014) catalogues the Committee's opinions on technology. In that opinion, we considered whether a law firm could provide its lawyers with remote access to its electronic files. We concluded that a law firm could use remote access "as long as it takes reasonable steps to ensure that confidential information is maintained." *Id.* ¶12

7. Similarly, in N.Y. State 842 (2010), which considered the use of cloud data storage, we concluded that a lawyer could use this technology to store client records provided that the lawyer takes reasonable care to protect the client's confidential information. We also reached a similar conclusion in N.Y. State 939 (2012) as to the issue of lawyers from different firms sharing a computer system.

8. The concerns presented by the current inquiry were also present in N.Y. State 1019, N.Y. State 939 and N.Y. State 842, and those opinions govern the outcome here. That is, the inquirer may use the proposed technology provided that the lawyer takes reasonable steps to ensure that confidential information is not breached.[2] The inquirer must, for example, try to ensure that only authorized parties have access to the system on which the information is shared. Because of the fact-specific and evolving nature of technology, we do not purport to specify in detail the steps that will constitute reasonable care in any given set of circumstances. *See* N.Y. State 1019. ¶10. We note, however, that use of electronically stored information may not only require reasonable care to protect that information under Rule 1.6, but may also, under Rule 1.1, require the competence to determine and follow a set of steps that will constitute such reasonable care.[3]

9. Finally, we note that Rule 1.6 provides an exception to confidentiality rules based on a client's informed consent. Thus, as quoted in paragraph 5 above, a client may agree to the use of a technology that would otherwise be prohibited by the Rule. But as we have previously pointed out, "before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is 'informed' within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision." N.Y. State 1019 ¶11.

CONCLUSION

10. Whether a lawyer for a party in a transaction may post and share documents using a "cloud" data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

(17-14)

[1]Rule 1.6(a) defines "confidential information" generally to include "information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

[2]This result is consistent with results in other jurisdictions that have considered lawyers' use of off-site, third-party cloud services for storing and sharing documents. *See, e.g.,* ABA 95-398; Arizona Opinion 05-04; California Opinion 2010-179; Connecticut Inf. Opinion 2013-07; Florida Opinion 12-3 (2013); Illinois Opinion 10-01 (2009); Iowa Opinion 11-01; Maine Opinion 207 (2013); Massachusetts Opinion 12-03; Massachusetts Opinion 05-04; Missouri Inf. Opinion 2006-0092; Nebraska Opinion 06-05; New Hampshire Opinion 2012-13/4 (2013); New Jersey Opinion 701 (2006); North Carolina Opinion 2011-6 (2012); North Dakota Opinion 99-03 (1999); Ohio Opinion 2013-03; Oregon Opinion 2011-188; Pennsylvania Opinion 2011-200; Pennsylvania Opinion 2010-060; Vermont Opinion 2010-6 (2012); Washington Inf. Opinion 2215 (2012).

[3]It has been said for example that the duty of competence may require litigators, depending on circumstances, to possess a basic or even a more refined understanding of electronically stored information. *See, e.g*., Zachary Wang, "Ethics and Electronic Discovery: New Medium, Same Problems," 75 Defense Counsel Journal 328, at 7 (October 2008) ("disclosure of privileged information as a result of a lack of knowledge of a client's IT system would subject an attorney to discipline under Rules 1.1 and 1.6"). The California State Bar Standing Committee on Professional Responsibility and Conduct has tentatively approved an interim opinion interpreting California ethical rules as follows:

> Attorney competence related to litigation generally requires, at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, i.e., the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a given matter and the nature of the ESI involved. … An attorney lacking the required competence for the e-discovery issues in the case at issue has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation.

COPRAC Proposed Formal Opinion 11-0004 (2014).

New York State

Standardized

DOMESTIC INCIDENT REPORT (DIR)

(Form 3221-03/2016)

REMEMBER: Whenever possible, ask complainant the DIR questions OUT of earshot and eyesight of suspect

TIPS FOR COMPLETION

When completing the DIR please be sure:

- **To print legibly and firmly**
- Wraparound cover is in place
- All copies of each page are lined up properly
- Writing is visible on all 3 copies of the form
- To complete every section of the DIR
- To hand Victim Rights Notice to the victim
- Victim understands the Victim Rights Notice
- Victim receives all pink copies at the scene

WHERE TO SEND DIR FORMS

New York City (NYC) DIR forms are sent to NYPD and do not need to be sent directly to DCJS.

State Police forward DCJS copies of DIR to **Zone Headquarters.**

All Other Agencies, send DCJS copies of DIR to:
NYS Division of Criminal Justice Services
NYS Identification Bureau-DIR, 5th Floor
80 South Swan Street
Albany, New York 12210

If Suspect is on Probation or Parole Supervision, photocopy the **police copy** of DIR and send to the County Probation Department or the local Parole Office.

Addresses for County Probation Departments and Parole Offices can be found in the Criminal Justice Directory at: **http://criminaljustice.ny.gov**

HOW TO REQUEST MORE DIR FORMS

To order additional forms send an email to:

dcjs.dl.dirform@dcjs.ny.gov

When ordering forms, please provide the **agency name** and **street address** for shipment, no P.O. Boxes accepted. DIR forms come 25 forms to a pad. Please base your order on the **number of pads** needed, not the number of forms.

IMPORTANT HOTLINE NUMBERS

NYS Domestic and Sexual Violence	1-800-942-6906
Child Protective Services (Public)	1-800-342-3720
CPS (Mandated Reporter)	1-800-635-1522
Adult Protective Services	1-800-342-3009 (Option 6)

Local Service Provider Name:_____

Hotline:_____

Quick Reference Guide

Recommended Wording

(PRIOR DV HISTORY?) *"Has _____ ever hurt you, threatened harm to you or others, made you afraid, or forced you to do something that you didn't want to do (prior to this incident)?"*

(VICTIM FEARFUL?) "*Are you currently concerned or in **fear** for your safety or the safety of someone else because of _____'s behavior?"* (***Note:*** **Document specific fear and reasons for it. Fear may be an element of an offense** (e.g. menacing, coercion, stalking, etc.). Also, document in statement of allegations.

INFORM VICTIM. "*A **victim advocate can help you with SAFETY PLANNING,** an important issue to be discussed with a local service provider. On the back of a form that I will give you are some phone numbers that can assist you. **Do you need assistance with making arrangements for transportation to another location?"*** **Note: CPL 530.11(6) requires a police officer to advise a victim of local available services.)**

Officers are NOT required to arrest each person in dual complaint situations.

Officers must identify the PRIMARY PHYSICAL AGGRESSOR. Consider injuries, threats of past and future harm, history of domestic violence, and self-defense responses. An ARREST DECISION shall NOT be based on the willingness of a person to testify or participate in a judicial proceeding (*refer to the Primary/Dominant Aggressor Law, (CPL 140.10 (4)(c)).*

Below is a list of some frequently seen offenses in domestic violence incidents.

REMEMBER to CHARGE all relevant offenses and charge at the highest degree appropriate for the circumstances.

Family Offenses

(refer to CPL articles 140 and 530.11)

Aggravated Family Offense (240.75; E Felony)

Aggravated Harassment 2nd (240.30; A Misd.)

Assault 2nd (120.05; D Felony)
Assault 3rd (120.00; A Misdemeanor)
Attempted Assault (110.00)

Criminal Mischief 1st (145.12; B Felony)
Criminal Mischief 2nd (145.10; D Felony)
Criminal Mischief 3rd (145.05; E Felony)
Criminal Mischief 4th (145.00; A Misdemeanor)

Disorderly Conduct (240.20; Violation)
Forcible Touching (130.52; A Misdemeanor)

Harassment 1st (240.25; B Misdemeanor)
Harassment 2nd (240.26; Violation)

Menacing 2nd (120.14; A Misdemeanor)
Menacing 3rd (120.15; B Misdemeanor)

Reckless Endangerment 1st (120.25; D Felony)
Reckless Endangerment 2nd (120.20; A Misd.)

Sexual Abuse 2nd (130.60(1); A Misdemeanor)
Sexual Abuse 3rd (130.55; B Misdemeanor)
Sexual Misconduct (130.20; A Misd.)
Stalking 1st (120.60; D Felony)
Stalking 2nd (120.55; E Felony)
Stalking 3rd (120.50; A Misdemeanor)
Stalking 4th (120.45; B Misdemeanor)

Criminal Obstruction of Breathing or Blood Circulation (121.11; A Misd.)
Strangulation 1st (121.13; C Felony)
Strangulation 2nd (121.12; D Felony)

Coercion 2nd (135.60(1) (2) (3); A Misd.)

Grand Larceny 3rd (155.35; D Felony)
Grand Larceny 4th (155.30; E Felony)

Identity Theft 1st (190.80; D Felony)
Identity Theft 2nd (190.79; E Felony)
Identity Theft 3rd (190.78; A Misdemeanor)

Often Committed Offenses

Agg. Assault Person under 11 (120.12; E Felony)
Agg. Criminal Contempt (215.52; D Felony)
Agg. Harassment 1st (240.31; E Felony)
Aggravated Cruelty to Animals (NY Agg. & M Section 353-a; Felony)
Assault 1st (120.10; B Felony)
Burglary 1st (140.30; B Felony)
" 2nd (140.25; C Felony)
" 3rd (140.20; D Felony)
Robbery 1st (160.15; B Felony)
" 2nd (160.10; C Felony)
Coercion 1st (135.65; D Felony)
Criminal Contempt 1st (215.51; E Felony)
" 2nd (215.50; A Misdemeanor)
Criminal Trespass 1st (140.17; D Felony)
" 2nd (140.15; A Misdemeanor)
" 3rd (140.10; B Misdemeanor)
Endangering Welfare of Child (260.10; A Misd.)
Endang. Welf. of Vulnerable Elderly Person 1st (260.34; D Felony)
Intimidating Victim or Witness 1st (215.17; B Felony)
Intimidating Victim or Witness 2nd (215.16; D Felony)
Intimidating Victim or Witness 3rd (215.15; E Felony)
Menacing 1st (120.13; E Felony)
Manslaughter 1st (125.20; B Felony)
Manslaughter 2nd (125.15; C Felony)
Murder 1st (125.27; A-I Felony)
Murder 2nd (125.25; A-I Felony)
Resisting Arrest (205.30; A Misdemeanor)
Unlawful Imprisonment 1st (135.10; E Felony)
" 2nd (135.05; A Misd.)

Other Possible Offenses

Aggravated Sexual Abuse 1st (130.70; B Felony)
" 2nd (130.67; C Felony)
" 3rd (130.66; D Felony)
" 4th (130.65-a; E Felony)
Computer Tampering 1st (156.27; C Felony)
" 2nd (156.26; D Felony)
" 3rd (156.25; E Felony)
" 4th (156.20; A Misdemeanor)
Computer Trespass (156.10; E Felony)
Criminal Possession of a Dangerous Weapon 1st (265.04; B Felony)
Criminal Possession of a Weapon 2nd (265.03; C Felony)
" 3rd (265.02; D Felony)
" 4th (265.01; A Misd.)
Criminal Sexual Act 1st (130.50; B Felony)
" 2nd (130.45; D Felony)
" 3rd (130.40; E Felony)
Criminal Tampering 1st (145.20; D Felony)
" 2nd (145.15; A Misdemeanor)
" 3rd (145.14; B Misdemeanor)
Criminal Use of a Firearm 1st (265.09; B Felony)
" 2nd (265.08; A Misd.)
Criminally Negligent Homicide (125.10;E Felony)
Endang. Welf. Vulner. Elderly 2nd (260.32; E Fel)
Facil. a Sex Off. W. a Cont. Sub. (130.90; D Fel)
Kidnapping 1st (135.25; A-I Felony)
" 2nd (135.20; B Felony)
Rape 1st (130.35; B Felony)
" 2nd (130.30; D Felony)
" 3rd (130.25; E Felony)
Reckless Endanger. of Property (145.25; B Misd.)
Sexual Abuse 1st (130.65; D Felony)
Tampering with a Witness 1st (215.13; B Felony)
" 2nd (215.12; D Felony)
" 3rd (215.11; E Felony)
" 4th (215.10; A Misd.)
Unauth. Use of a Vehicle 1st (165.08; D Felony)
" 2nd (165.06; E Felony)
" 3rd (165.05; A Misd.)

Unlawful Surveillance 2nd (250.45; E Felony)

Incident

Agency: | **A** | **New York State DOMESTIC INCIDENT REPORT** | ORI: | Incident #

Reported Date (MM/DD/YYYY) | Time (24 hours) | Occurred Date (MM/DD/YYYY) | Time (24 hours) | ☐ Officer Initiated ☐ Radio Run ☐ Walk-in ☐ ICAD (NYC) | Complaint #

Address (Street No., Street Name, Bldg. No., Apt No.) | City, State, Zip

Victim (P1)

Name (Last, First, M.I.) (Include Aliases) | DOB (MM/DD/YYYY) | Age: | ☐ Female ☐ Male ☐ Self-Identified:

Address (Street No., Street Name, Bldg. No., Apt No.) | Victim Phone Number: | Language:

City, State, Zip | ☐ White ☐ Black ☐ Asian ☐ American Indian ☐ Other | ☐ Hispanic ☐Non Hispanic ☐Unknown

How can we safely contact you? (i.e. Name, Phone, Email) | ☐ Other Identifier:

Suspect (P2)

Name (Last, First, M.I.) (Include Aliases) | DOB (MM/DD/YYYY) | Age: | ☐ Female ☐ Male ☐ Self-Identified:

Address (Street No., Street Name, Bldg. No., Apt No.) | Suspect Phone Number: | Language:

City, State, Zip | ☐ White ☐ Black ☐ Asian ☐ American Indian ☐ Other | ☐ Hispanic ☐ Non Hispanic ☐Unknown ☐ Other Identifier:

Do suspect and victim live together ? ☐ Yes ☐ No | Suspect/P2 present? ☐ Yes ☐ No | Was suspect injured? ☐ Yes ☐ No If yes describe: | Possible drug or alcohol use? ☐ Yes ☐ No | Suspect supervised? ☐ Probation ☐ Parole ☐ Not Supervised ☐ Status Unknown

Suspect (P2) Relationship to Victim (P1) ☐ Married ☐ Intimate Partner/Dating ☐ Formerly Married ☐ Former Intimate Partner ☐ Parent of Victim (P1) ☐ Child of Victim ☐ Relative: _____ ☐ Other: _____ | Do the suspect and victim have a child in common? ☐ Yes ☐ No

Victim Interview

Emotional condition of **VICTIM?** ☐ Upset ☐ Nervous ☐ Crying ☐ Angry ☐ Other:

What were the first words that **VICTIM** said to the Responding Officers at the scene regarding the incident?

Did suspect make victim fearful? ☐ Yes ☐ No If yes, describe:

Weapon Used? ☐ Yes ☐ No Gun: ☐ Yes ☐ No Other, describe:

Access to Guns? ☐ Yes ☐ No If yes, describe:

Suspect Threats? ☐ Yes ☐ No If Yes, Threats to: ☐ Victim ☐ Child(ren) ☐ Pet ☐ Commit Suicide ☐ Other Describe:

Injured? ☐ Yes ☐ No If yes, describe:

In Pain ? ☐ Yes ☐ No If yes, describe:

Strangulation? ☐ Yes ☐ No ☐ Loss of Consciousness ☐ Urination/Defecation ☐ Red eyes/Petechia ☐ Sore Throat ☐ Breathing Changed ☐ Difficulty Swallowing

Visible Marks? ☐ Yes ☐ No If yes, describe:

Suspect

What did the **SUSPECT** say (Before and After Arrest) :

710.30 completed? ☐ Yes ☐ No

Witnesses

Child/Witness (1) Name (Last, First, M.I.)	DOB:	Child/Witness(1) Address (Street No., Name, Bldg./Apt)	City, State, Zip	Phone:
Child/Witness (2) Name (Last, First, M.I.)	DOB:	Child/Witness(2) Address (Street No., Name, Bldg./Apt)	City, State, Zip	Phone:

Incident Narrative

Briefly describe the circumstances of this incident:

DIR Repository checked? ☐ Yes ☐ No | Order of Protection Registry checked? ☐ Yes ☐ No | Order of Protection in effect? ☐ Yes ☐ No ☐ Refrain ☐ Stay Away

Evid

Evidence Present? ☐ Yes ☐ No | **Photos taken:** ☐ Victim Injury ☐ Suspect Injury ☐ Other: | **Other Evidence:** ☐ Damaged Property ☐ Videos ☐ Electronic Evidence ☐ Other: | **Destruction of Property?** ☐ Yes ☐ No If yes, Describe:

Offense

Offense Committed? ☐ Yes ☐ No | Was suspect arrested? ☐ Yes ☐ No If no, explain: | Offense 1 | Law (e.g. PL) | Offense 2 | Law (e.g. PL)

Incident

Agency: | **A** | **New York State DOMESTIC INCIDENT REPORT** | ORI: | Incident #

Reported Date (MM/DD/YYYY) | Time (24 hours) | Occurred Date (MM/DD/YYYY) | Time (24 hours) | ☐ Officer Initiated ☐ Radio Run ☐ Walk-in ☐ ICAD (NYC) | Complaint #

Address (Street No., Street Name, Bldg. No., Apt No.) | City, State, Zip

Victim (P1)

Name (Last, First, M.I.) (Include Aliases) | DOB (MM/DD/YYYY) | Age: | ☐ Female ☐ Male ☐ Self-Identified:

Address (Street No., Street Name, Bldg. No., Apt No.) | Victim Phone Number: | Language:

City, State, Zip | ☐ White ☐ Black ☐ Asian ☐ American Indian ☐ Other | ☐ Hispanic ☐Non Hispanic ☐Unknown

How can we safely contact you? (i.e. Name, Phone, Email) | ☐ Other Identifier:

Suspect (P2)

Name (Last, First, M.I.) (Include Aliases) | DOB (MM/DD/YYYY) | Age: | ☐ Female ☐ Male ☐ Self-Identified:

Address (Street No., Street Name, Bldg. No., Apt No.) | Suspect Phone Number: | Language:

City, State, Zip | ☐ White ☐ Black ☐ Asian ☐ American Indian ☐ Other | ☐ Hispanic ☐ Non Hispanic ☐Unknown

☐ Other Identifier:

Do suspect and victim live together ? ☐ Yes ☐ No | Suspect/P2 present? ☐ Yes ☐ No | Was suspect injured? ☐ Yes ☐ No If yes describe: | Possible drug or alcohol use? ☐ Yes ☐ No | Suspect supervised? ☐ Probation ☐ Parole ☐ Not Supervised ☐ Status Unknown

Suspect (P2) Relationship to Victim (P1) ☐ Married ☐ Intimate Partner/Dating ☐ Formerly Married ☐ Former Intimate Partner ☐ Parent of Victim (P1) ☐ Child of Victim ☐ Relative: _____ ☐ Other: _____ | Do the suspect and victim have a child in common? ☐ Yes ☐ No

Victim Interview

Emotional condition of **VICTIM?** ☐ Upset ☐ Nervous ☐ Crying ☐ Angry ☐ Other:

What were the first words that **VICTIM** said to the Responding Officers at the scene regarding the incident?

Did suspect make victim fearful? ☐ Yes ☐ No If yes, describe:

Weapon Used? ☐ Yes ☐ No Gun: ☐ Yes ☐ No Other, describe:

Access to Guns? ☐ Yes ☐ No If yes, describe:

Suspect Threats? ☐ Yes ☐ No If Yes, Threats to: ☐ Victim ☐ Child(ren) ☐ Pet ☐ Commit Suicide ☐ Other Describe:

Injured? ☐ Yes ☐ No If yes, describe:

In Pain ? ☐ Yes ☐ No If yes, describe:

Strangulation? ☐ Yes ☐ No ☐ Loss of Consciousness ☐ Urination/Defecation ☐ Red eyes/Petechia ☐ Sore Throat ☐ Breathing Changed ☐ Difficulty Swallowing

Visible Marks? ☐ Yes ☐ No If yes, describe:

Suspect

What did the **SUSPECT** say (Before and After Arrest) :

710.30 completed? ☐ Yes ☐ No

Witnesses

Child/Witness (1) Name (Last, First, M.I.)	DOB:	Child/Witness(1) Address (Street No., Name, Bldg./Apt)	City, State, Zip	Phone:
Child/Witness (2) Name (Last, First, M.I.)	DOB:	Child/Witness(2) Address (Street No., Name, Bldg./Apt)	City, State, Zip	Phone:

Incident Narrative

Briefly describe the circumstances of this incident:

DIR Repository checked? ☐ Yes ☐ No | Order of Protection Registry checked? ☐ Yes ☐ No | Order of Protection in effect? ☐ Yes ☐ No ☐ Refrain ☐ Stay Away

Evid

Evidence Present? ☐ Yes ☐ No | **Photos taken:** ☐ Victim Injury ☐ Suspect Injury ☐ Other: | **Other Evidence:** ☐ Damaged Property ☐ Videos ☐ Electronic Evidence ☐ Other: | **Destruction of Property?** ☐ Yes ☐ No If yes, Describe:

Offense

Offense Committed? ☐ Yes ☐ No	Was suspect arrested? ☐ Yes ☐ No If no, explain:	Offense 1	Law (e.g. PL)	Offense 2	Law (e.g. PL)

Incident

Agency: | **A** | **New York State DOMESTIC INCIDENT REPORT** | Incident #

Reported Date (MM/DD/YYYY) | Time (24 hours) | Occurred Date (MM/DD/YYYY) | Time (24 hours) | ☐ Officer Initiated ☐ Radio Run ☐ Walk-in ☐ ICAD (NYC) | Complaint #

Address (Street No., Street Name, Bldg. No., Apt No.) | City, State, Zip

Suspect (P2)

Name (Last, First, M.I.) (Include Aliases) | DOB (MM/DD/YYYY) | Age: | ☐ Female ☐ Male ☐ Self-Identified:

Address (Street No., Street Name, Bldg. No., Apt No.) | Suspect Phone Number: | Language:

City, State, Zip | ☐ White ☐ Black ☐ Asian ☐ American Indian ☐ Other | ☐ Hispanic ☐ Non Hispanic ☐ Unknown ☐ Other Identifier:

Do suspect and victim live together ? ☐ Yes ☐ No | Suspect/P2 present? ☐ Yes ☐ No | Was suspect injured? ☐ Yes ☐ No If yes describe: | Possible drug or alcohol use? ☐ Yes ☐ No | Suspect supervised? ☐ Probation ☐ Parole ☐ Not Supervised ☐ Status Unknown

Suspect (P2) Relationship to Victim (P1) ☐ Married ☐ Intimate Partner/Dating ☐ Formerly Married ☐ Former Intimate Partner ☐ Parent of Victim (P1) ☐ Child of Victim ☐ Relative: _____ ☐ Other: _____ | Do the suspect and victim have a child in common? ☐ Yes ☐ No

Victim Interview

Emotional condition of **VICTIM?** ☐ Upset ☐ Nervous ☐ Crying ☐ Angry ☐ Other:

What were the first words that **VICTIM** said to the Responding Officers at the scene regarding the incident?

Did suspect make victim fearful? ☐ Yes ☐ No If yes, describe:

Weapon Used? ☐ Yes ☐ No Gun: ☐ Yes ☐ No Other, describe:

Access to Guns? ☐ Yes ☐ No If yes, describe:

Suspect Threats? ☐ Yes ☐ No If Yes, Threats to: ☐ Victim ☐ Child(ren) ☐ Pet ☐ Commit Suicide ☐ Other Describe:

Injured? ☐ Yes ☐ No If yes, describe:

In Pain ? ☐ Yes ☐ No If yes, describe:

Strangulation? ☐ Yes ☐ No ☐ Loss of Consciousness ☐ Urination/Defecation ☐ Red eyes/Petechia ☐ Sore Throat ☐ Breathing Changed ☐ Difficulty Swallowing

Visible Marks? ☐ Yes ☐ No If yes, describe:

Suspect

What did the **SUSPECT** say (Before and After Arrest) :

710.30 completed? ☐ Yes ☐ No

Incident Narrative

Briefly describe the circumstances of this incident:

DIR Repository checked? ☐ Yes ☐ No | Order of Protection Registry checked? ☐ Yes ☐ No | Order of Protection in effect? ☐ Yes ☐ No ☐ Refrain ☐ Stay Away

Evid

Evidence Present? ☐ Yes ☐ No | **Photos taken:** ☐ Victim Injury ☐ Suspect Injury ☐ Other: | **Other Evidence:** ☐ Damaged Property ☐ Videos ☐ Electronic Evidence ☐ Other: | **Destruction of Property?** ☐ Yes ☐ No If yes, Describe:

Offense

Offense Committed? ☐ Yes ☐ No | Was suspect arrested? ☐ Yes ☐ No If no, explain: | Offense 1 | Law (e.g. PL) | Offense 2 | Law (e.g. PL)

Agency:	B	ORI:	Incident #	Complaint #

Prior History

Describe Victim's prior domestic incidents with this suspect (Last, Worst, First):

If the Victim answers "yes" to any questions in this box refer to the NYS Domestic and Sexual Violence Hotline at 1-800-942-6906 or Local Domestic Violence Service Provider: ( ) _____.

Has Suspect ever:

Threatened to kill you or your children? ☐ Yes ☐ No

Strangled or "choked" you? ☐ Yes ☐ No

Beaten you while you were pregnant? ☐ Yes ☐ No

Is suspect capable of killing you or children? ☐ Yes ☐ No

Is suspect violently and constantly jealous of you? ☐ Yes ☐ No

Has the physical violence increased in frequency or severity over the past 6 months? ☐ Yes ☐ No

Is there reasonable cause to suspect a child may be the victim of abuse, neglect, maltreatment or endangerment? ☐ Yes ☐ No

If Yes, the Officer must contact the **NYS Child Abuse Hotline Registry # 1-800-635-1522.**

Was DIR given to the Victim at the scene? ☐ Yes ☐ No if **NO**, Why:

Was Victim Rights Notice given to the Victim? ☐ Yes ☐ No if **NO**, Why:

Signatures:

Reporting Officer (Print and Sign include Rank and ID#)

Supervisor (Print and Sign include Rank and ID#)

STATEMENT OF ALLEGATIONS/SUPPORTING DEPOSITION

* Officers are encouraged to assist the Victim in completing this section of the form.

Suspect Name (Last, First, M.I)

I _____(Victim/Deponent Name) state that on _____ / ____ / _____, (Date)

at _____ (Location of incident) in the County/City/Town/Village _____

_____of the State of New York, the following did occur: _____

(Use additional page as needed)

False Statements made herein are punishable as a Class A Misdemeanor, pursuant to section 210.45 of the Penal Law.

Victim/Deponent Signature _____ Date _____

Witness or Officer Signature _____ Date _____

Interpreter Signature and Interpreter Service Provider Name _____ Date _____

Interpreter Requested ☐ Yes ☐ No Interpreter Used ☐ Yes ☐ No

Note:

Whether or not this form is signed, this DIR Form will be filed with Law Enforcement.

Page ____ Of ____

Agency:	B	ORI:	Incident #	Complaint #

Prior History

Describe Victim's prior domestic incidents with this suspect (Last, Worst, First):

If the Victim answers "yes" to any questions in this box refer to the NYS Domestic and Sexual Violence Hotline at 1-800-942-6906 or Local Domestic Violence Service Provider: ( ) _____.

Has Suspect ever:

Threatened to kill you or your children? ☐ Yes ☐ No

Strangled or "choked" you? ☐ Yes ☐ No

Beaten you while you were pregnant? ☐ Yes ☐ No

Is suspect capable of killing you or children? ☐ Yes ☐ No

Is suspect violently and constantly jealous of you? ☐ Yes ☐ No

Has the physical violence increased in frequency or severity over the past 6 months? ☐ Yes ☐ No

Is there reasonable cause to suspect a child may be the victim of abuse, neglect, maltreatment or endangerment? ☐ Yes ☐ No

If Yes, the Officer must contact the **NYS Child Abuse Hotline Registry # 1-800-635-1522.**

Was DIR given to the Victim at the scene? ☐ Yes ☐ No if **NO**, Why:

Was Victim Rights Notice given to the Victim? ☐ Yes ☐ No if **NO**, Why:

Signatures:

Reporting Officer (Print and Sign include Rank and ID#)

Supervisor (Print and Sign include Rank and ID#)

STATEMENT OF ALLEGATIONS/SUPPORTING DEPOSITION

* Officers are encouraged to assist the Victim in completing this section of the form.

Suspect Name (Last, First, M.I)

I _____(Victim/Deponent Name) state that on _____ / ____ / _____, (Date)

at _____ (Location of incident) in the County/City/Town/Village _____

_____of the State of New York, the following did occur: _____

(Use additional page as needed)

False Statements made herein are punishable as a Class A Misdemeanor, pursuant to section 210.45 of the Penal Law.

Victim/Deponent Signature _____ Date _____

Witness or Officer Signature _____ Date _____

Interpreter Signature and Interpreter Service Provider Name _____ Date _____

Interpreter Requested ☐ Yes ☐ No Interpreter Used ☐ Yes ☐ No

Note:

Whether or not this form is signed, this DIR Form will be filed with Law Enforcement.

Page ____ Of ____

Agency:	B [redacted]	Incident #	Complaint #

Prior History

Describe Victim's prior domestic incidents with this suspect (Last, Worst, First):

If the Victim answers "yes" to any questions in this box refer to the NYS Domestic and Sexual Violence Hotline at 1-800-942-6906 or Local Domestic Violence Service Provider: ( ) _____.

Has Suspect ever:

Threatened to kill you or your children? ☐ Yes ☐ No

Strangled or "choked" you? ☐ Yes ☐ No

Beaten you while you were pregnant? ☐ Yes ☐ No

Is suspect capable of killing you or children? ☐ Yes ☐ No

Is suspect violently and constantly jealous of you? ☐ Yes ☐ No

Has the physical violence increased in frequency or severity over the past 6 months? ☐ Yes ☐ No

Is there reasonable cause to suspect a child may be the victim of abuse, neglect, maltreatment or endangerment? ☐ Yes ☐ No

If Yes, the Officer must contact the **NYS Child Abuse Hotline Registry # 1-800-635-1522.**

Was DIR given to the Victim at the scene? ☐ Yes ☐ No if **NO**, Why:

Was Victim Rights Notice given to the Victim? ☐ Yes ☐ No if **NO**, Why:

Signatures:

Reporting Officer (Print and Sign include Rank and ID#)

Supervisor (Print and Sign include Rank and ID#)

STATEMENT OF ALLEGATIONS/SUPPORTING DEPOSITION

* Officers are encouraged to assist the Victim in completing this section of the form.

Suspect Name (Last, First, M.I)

I _____(Victim/Deponent Name) state that on _____ / ____ / _____, (Date)

at _____ (Location of incident) in the County/City/Town/Village _____

_____of the State of New York, the following did occur: _____

(Use additional page as needed)

False Statements made herein are punishable as a Class A Misdemeanor, pursuant to section 210.45 of the Penal Law.

Victim/Deponent Signature _____ Date _____

Witness or Officer Signature _____ Date _____

Interpreter Signature and Interpreter Service Provider Name _____ Date _____

Interpreter Requested ☐ Yes ☐ No Interpreter Used ☐ Yes ☐ No

Note:

Whether or not this form is signed, this DIR Form will be filed with Law Enforcement.

Page ____ Of ____

IF YOU ARE THE VICTIM OF DOMESTIC VIOLENCE, THE POLICE AND COURTS CAN HELP.

What the Police Can Do:

*Assist you with finding a safe place, a place away from the violence.
*Inform you about how the court can help protect you from the violence.
*Help you and your children get medical care for any injuries you received.
*Assist you in getting necessary belongings from your home.
*Provide you with copies of police reports about the violence.
*File a complaint in criminal court, and tell you where your local criminal and family courts are located.

What the Courts Can Do:

*If the person who harmed you or threatened you is a relative by blood or marriage, or is someone you've had a child with, or is someone with whom you are or have had an intimate relationship, then you have the right to take your case to family court, criminal court or both.
*The forms you need are available from the family court and the criminal court.
*The courts can decide to provide a temporary order of protection for you, your children and any witnesses who may request one.
*The family court may appoint a lawyer to help you if the court finds that you cannot afford one.
*The family court may order temporary child support and temporary custody of your children.

New York Law States: If you are the victim of domestic violence, you may request that the officer assist in providing for your safety and that of your children, including providing information on how to obtain a temporary order of protection. You may also request that the officer assist you in obtaining your essential personal effects and locating and taking you, or assist in making arrangements to take you, and your children to a safe place within such officer's jurisdiction, including but not limited to a domestic violence program, a family member's or a friend's residence, or a similar place of safety. When the officer's jurisdiction is more than a single county, you may ask the officer to take you or make arrangements to take you and your children to a place of safety in the county where the incident occurred. If you or your children are in need of medical treatment, you have the right to request that the officer assist you in obtaining such medical treatment. You may request a copy of any incident reports at no cost from the law enforcement agency. You have the right to seek legal counsel of your own choosing and if you proceed in family court and if it is determined that you cannot afford an attorney, one must be appointed to represent you without cost to you. You may ask the district attorney or a law enforcement officer to file a criminal complaint. You also have the right to file a petition in the family court when a family offense has been committed against you. You have the right to have your petition and request for an order of protection filed on the same day you appear in court, and such request must be heard that same day or the next day court is in session. Either court may issue an order of protection from conduct constituting a family offense which could include, among other provisions, an order for the respondent or defendant to stay away from you and your children. The family court may also order the payment of temporary child support and award temporary custody of your children. If the family court is not in session, you may seek immediate assistance from the criminal court in obtaining an order of protection. The forms you need to obtain an order of protection are available from the family court and the local criminal court. The resources available in this community for information relating to domestic violence, treatment of injuries, and places of safety and shelters can be accessed by calling the following 800 numbers. Filing a criminal complaint or a family court petition containing allegations that are knowingly false is a crime. *(NYS Criminal Procedure Law, Section 530.11 (6))*

NEW YORK STATE
24 HOUR DOMESTIC AND SEXUAL VIOLENCE HOTLINE
1-800-942-6906
English and Español, Multi-language Accessibility
National Relay Service for Deaf or Hard of Hearing:711

NEW YORK CITY (all languages)
1-800-621-Hope (4673) or 311

COURT INFORMATION

New York City—Criminal Court Information
1-646-386-4500

To obtain court information for other areas of NYS, ask the responding officer for court numbers, consult your phone directory, or call the Domestic and Sexual Violence Hotline (1-800-942-6906)

VICTIM INFORMATION AND NOTIFICATION EVERYDAY (VINE)

Victims may receive information relating to the status and release dates of persons incarcerated in state prison or local jails in New York State. For more information on this program and how you can register, call

1-888-VINE-4NY (1-888-846-3469) or www.vinelink.com

STATEWIDE AUTOMATED VICTIM INFORMATION AND NOTIFICATION (SAVIN-NY)

Victim notification program which allows domestic violence victims to register to be notified when an Order of Protection has been served
www.nyalert.gov

Si USTED ES VÍCTIMA DE VIOLENCIA DOMÉSTICA, PUEDEN AYUDAR LA POLICÍA Y LOS TRIBUNALES.

Lo que puede hacer la policía:

* Ayudarle a encontrar un lugar seguro, un lugar lejos de la violencia.
* Informarle cómo la corte puede ayudar a protegerle de la violencia.
* Ayudarle a obtener atención médica para heridas o lesiones que usted y sus hijos pudieran haber sufrido.
* Ayudarle a sacar de su hogar las pertenencias necesarias.
* Proveerle copias de informes de la policía sobre la violencia.
* Presentar una querella ante el tribunal en lo penal e informarle sobre la localización del tribunal en lo penal y del tribunal de familia en su comunidad.

Lo que pueden hacer los tribunales:

*Si la persona que le hizo daño o que lo amenazó es su pariente o familiar político, o es alguien con quien usted tuvo un hijo, alguien con quien usted tiene o ha tenido una relación íntima, entonces usted tiene el derecho de llevar el caso al tribunal de familia, en lo penal, o ambos.
*Puede obtener los formularios que necesita en el tribunal de familia y en el tribunal en lo penal.
*Los tribunales podrían proveerle una orden de protección provisional para usted, sus hijos, y cualquier testigo que así lo pida.
*Si el tribunal determina que usted no puede pagar los servicios de un abogado, el tribunal puede asignarle uno.
*El tribunal de familia puede otorgarle manutención provisional para sus hijos, así como la custodia provisional de sus hijos.

La Ley de Nueva York establece que: Si usted es víctima de violencia doméstica, puede pedirle al oficial de la policía que resguarde su seguridad y la de sus hijos. Incluso, puede pedirle que le proporcione información sobre cómo obtener una orden temporal de protección. Asimismo, puede solicitar que dicho oficial de la policía le ayude a obtener sus efectos personales esenciales y a localizar un lugar seguro, al igual que transportarle a usted y a sus hijos a dicho lugar, o ayudarle a hacer arreglos para obtener dicha transportación dentro de la jurisdicción de dicho oficial de la policía, incluyendo pero sin limitarse a transportación a un programa que provea servicios contra la violencia doméstica, la residencia de un miembro de su familia o la residencia de un amigo, o un lugar que sea igualmente seguro. Cuando la jurisdicción de dicho oficial de la policía abarca más de un condado, usted puede pedirle al oficial que le transporte o que haga arreglos para transportarle a usted y a sus hijos a un lugar seguro en el condado donde ocurrió el incidente. Si usted o sus hijos necesitan tratamiento médico, usted tiene derecho a solicitar que dicho oficial de la policía le ayude a obtener dicho tratamiento médico. Usted puede solicitar que la agencia policial le provea una copia gratis de cualquier informe del incidente. Usted tiene derecho a buscar y escoger su propio consejero legal y si usted procede a utilizar el tribunal de familia y se determina que usted no puede pagar por los servicios de un abogado, uno deberá ser designado para que le represente sin costo para usted. Usted puede pedirle al fiscal de distrito o a un oficial de la policía que radique una querella penal. Usted también tiene derecho a presentar una petición ante el tribunal de familia cuando una ofensa de familia ha sido cometida contra usted. Usted tiene derecho a presentar dicha petición y a solicitar una orden de protección el mismo día que usted comparece en tribunales, y dicha petición debe ser vista el tribunal ese mismo día, o el próximo día en que esté en sesión. Cualquiera de los tribunales puede expedir una orden de protección un causa de una conducta que constituya una ofensa de familia, la cual puede incluir entre otras disposiciones, una orden contra el demandado o acusado que le requiera permanecer lejos de usted y de sus niños. El tribunal de familia también puede ordenar el pago temporal de manutención para sus niños y otorgarle a usted la custodia temporal de sus niños. Si el tribunal de familia no está en sesión, usted puede solicitar ayuda inmediata del tribunal en lo penal para obtener una orden de protección. Los formularios que usted necesita para obtener una orden de protección están disponibles en el tribunal de familia y en el tribunal en lo penal. Para acceso a los recursos disponibles en esta comunidad que proveen información sobre violencia doméstica, tratamiento de lesiones, y lugares seguros y refugios, llame a los siguientes números gratuitos. Es un delito radicar una querella penal o una petición ante el tribunal de familia, a sabiendas de que dicha querella o petición contiene alegaciones falsas. *(NYS Criminal Procedure Law, Section 530.11 (6))*

ESTADO DE NUEVA YORK
LÍNEAS DIRECTAS PARA VIOLENCIA DOMÉSTICA Y SEXUAL LAS 24 HORAS

1-800-942-6906
Ingles y Español, Multi-language Accessibility
Servicio de retransmisión nacional para sordos o con problemas de audición:711

CIUDAD DE NUEVA YORK (todo lenguajes)
1-800-621-Hope (4673) o 311

INFORMACIÓN DEL TRIBUNAL

La ciudad de Nueva York
Información de el tribunal de penal del condado
1-646-386-4500

Para obtener la información del tribunal para otras áreas de NYS, pedirle al official de la policía que responde los números del tribunal , consulte su guía de telefonos, o llame el teléfono de Ayuda contra la violencia doméstica y sexual (número de teléfono proporcionado arriba).

Información y Notificación Diaria Para La Víctima (VINE)

Las víctimas pueden recibir información relacionada con el estado y la fecha de excarcelación de personas encarceladas en prisiones estatales o en cárceles locales en el estado de Nueva York.
Para más información sobre este programa y como puede registrarse, llame al
1-888-VINE-4NY (1-888-846-3469) o www.vinelink.com

NOTIFICACIONES E INFORMACIÓN ESTATAL VÍCTIMA AUTOMATIZADO (SAVIN-NY)

Programa de notificación de la víctima que les permite a las víctimas de violencia doméstica registrarse para ser Notificadas cuando una Orden judicial de protección de la familia ha sido entregada
www.nyalert.gov

Incorporating Risk Assessment into the Courts: The Domestic Violence Risk Factor Guides for New York State Judges

By Rebecca Thomforde-Hauser, Associate Director, Domestic Violence Programs, Center for Court Innovation

In order to increase safety for victims, many criminal justice agencies have implemented risk assessment tools in domestic violence cases. However, few tools have been specifically designed for use by Courts. In order to address this gap, the Center for Court Innovation staff worked with the New York State Court System to consider how and where risk factors should be taken into account by the court. (Hyper link to https://www.ncjrs.gov/pdffiles1/nij/grants/209731.pdf for a summary of the research on risk factors and assessments.)

In 2012, with federal funding, project planners created an advisory group of judges and court personnel to meet with national experts, and review local and national best practices. Center staff then drafted a guide for judges that was reviewed by the advisory group and stakeholder agencies and piloted during the summer of 2013. (For more on the pilot project: http://www.courtinnovation.org/research/fact-sheet-erie-risk-assessment-pilot.) The pilot, conducted with Haven House, demonstrated positive effects on safety and effectiveness of protective orders.

The Domestic Violence Risk Factor Guide For Family Court Judges is two sided and includes a chart identifying risk factors, what information to look for in a petition, and New York Family Law specific to each of the factors. This guide was designed to support effective decision-making, not as an actuarial tool or a guide for questioning litigants. Guides were distributed statewide after training to family and matrimonial judges. A similar guide was created for matrimonial judges in 2014 and a guide for criminal court judges is in the process of being developed. For more information contact us at thomforr@courtinnovation.org.

This Guide is to assist Family Court judges in identifying domestic violence risk factors and to offer legal remedies or specific conditions that may be appropriate that respond to the correlating risk. This Guide may also be valuable in assisting courts in crafting temporary and final custody, parental access and visitation orders in cases involving domestic violence. The Guide is not exhaustive, is not meant to be a substitute for the court's discretion in determining the credibility of the allegations and weight of each factor, and is not meant to be filled out, scored in any way, or placed in any court file.

HOW TO USE - FAMILY COURT JUDICIAL GUIDE TO DOMESTIC VIOLENCE RISK FACTORS

GENERAL INSTRUCTIONS

- Provide both parties with notice of right to retain counsel and, if indigent, to assigned counsel under FCA 262(a)(ii) and 821-a(3)(a) and Jud L 35
- Provide the responding party with an opportunity to be heard as to any risk factors identified
- If ex parte application for a Temporary Order of Protection involves exclusion from the home, the case should be scheduled with a short return date
- **EXPLAIN THE TERMS AND CONDITIONS OF THE TEMPORARY ORDER OF PROTECTION TO ALL PARTIES, WITH THE ASSISTANCE OF AN INTERPRETER WHERE LIMITED ENGLISH PROFICIENCY OR HEARING IMPAIRMENT IS AN ISSUE**

Limitations of eliciting safety or risk information from petitioners in open court

- **Safety concerns or trauma** can affect the petitioner's ability to provide accurate information in open court
- **Soliciting information from petitioners** in a private setting (by someone other than the judge) improves the accuracy of information and also serves as an opportunity to provide information and resources to the petitioner

At Initial Hearing under §828:

- **This tool can assist in determining the terms and conditions** on the temporary order, whether to issue a warrant, how quickly to calendar the return hearing, and whether temporary support should be ordered

At Dispositional Hearings §833:

- **This tool can assist in determining type and length of order**, whether aggravating circumstances apply and which conditions are appropriate, including firearms surrender, support, children on the order, and/or program mandates

Requests for Modifications §154-c(2) and §844; Violation Hearings §846:

- **This tool can assist in modification of type and length of order**, and which conditions are appropriate, including firearms surrender, support, children on the order, and/or program mandates; or adding terms and conditions after a violation hearing

Provide petitioners information on risk assessment factors and the option of consulting with confidential advocates

- Information and access to advocates improves petitioner safety and the quality of petitioners' risk assessments and, as a result, the court's own risk assessments

Cultural factors may impact litigants' understanding of this tool

- Information and access to language services should be made available to litigants to ensure their understanding of the risk factors and the petition
- Some of the terms on this tool may need to be explained in more detail

Note that this list of risk factors is not exclusive

- The listed factors are the ones **most commonly present when the risk of serious harm or death exists**
- Additional factors exist which assist in prediction of re-assault
- Petitioners may face and fear other risks such as homelessness, poverty, criminal charges, loss of children or family supports

Remember that the level and type of risk can change over time

- **The most dangerous time is during or after the period when the petitioner:**
  - is separating or has separated from the respondent
  - has disclosed or is attempting to disclose the abuse to others

Risk factors may be used to tailor supervision strategies and oversight.

This Guide is an educational tool used to contextualize certain behaviors within the NY State Penal Code. It may also be valuable in assisting courts in making custody-related determinations in cases involving domestic violence.

REMEMBER TO EXPLAIN THE TERMS AND CONDITIONS OF THE TEMPORARY ORDER TO THE PETITIONER.

These factors were compiled based on the work of Minnesota's Gender Fairness Implementation Committee; 2009, Identifying Risk Worksheet created by Probation Officer James E. Henderson Jr. of the 15th District Court in Ann Arbor MI. This project was supported by subgrant No. VW10562640 and subgrant no.VW12562642 awarded pursuant to a S.T.O.P. Violence Against Women Formula Grant Program administered by DCJS, the New York State administering office. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the state or the U.S. Department of Justice, Office on Violence Against Women. This guide was developed by the Unified Court System with the assistance of the Center for Court Innovation. June 2015

New York State Unified Court System

FAMILY COURT JUDICIAL GUIDE TO DOMESTIC VIOLENCE RISK FACTORS

RISK FACTOR	WHAT TO LOOK FOR	LEGAL CONTEXT
Context of Violence	• Was this the **first time** that something like this happened? • If not, what happened before? How long ago? • What was the **worst or most serious thing** that happened? • Medical treatment needed? • Has the **physical violence increased** in frequency or severity over the past year? • Is there a recent **loss of employment**? • Is there a history of **substance abuse or mental health** concerns?	Use of some illegal drugs; increased severity/ frequency of violence; unemployment increases lethality and recidivism. Medical costs can be allocated FCA §828(4) and §842(h); batterer's program can be required, and may include substance abuse programs under §842(g).
Criminal and Family Court History	• **Criminal and Family Court check**, OP registry, sex offender registry • Pending or prior **Orders of Protection** • Pending order of **Support**	Prior OPs/crim history can be a risk factor for re-offending. FCA §814 provides for communication between Crim and Fam. Ct.; §822(6) OP inquiry required; prior orders and violations are relevant FCA §821-1(6); §FCA 827.
Relationship Status	• When did the relationship begin? When did it end? • Where does each party live? Did they live together, if so when? • Are they **recently separated**?	Separation within the past year increases risk of lethality and recidivism. FCA §828 authorizes temporary child support; FCA §842 and RPL §227-c authorize lease termination.
Firearms/ Weapons	• Does respondent have **access to a firearm or weapon**? • Is there a firearm or weapon in the home? • Has the respondent ever used or **threatened to use a weapon** against the petitioner?	Respondent access to firearm and use or threatened use of lethal weapon increases lethality risk. FCA §842-a and18 U.S.C. 922(g)(8,9) include firearms restrictions.
Strangulation	• Has respondent ever **attempted to strangle** or choke the petitioner?	Strangulation increases lethality. Obstruction of breathing PL §121.11/12/13.
Threats to Kill	• Has respondent ever **threatened to or tried to kill** the petitioner?	Disorderly Conduct, Harassment and Aggravated Harassment PL §240.20/25/26/30/31.
Sexual Violence	• Has respondent **forced the petitioner to have sex**?	PL Art 130 Sex Offenses.
Controlling Behavior	• Does respondent **try to control** most or all of petitioner's daily activities? • Is respondent **constantly or violently jealous**? • Who has **access to bank accounts**, the car, etc.?	Violent jealousy and stalking behaviors are lethality factors and may constitute Stalking PL §120.45-60.
Stalking	• Does the respondent **repeatedly call, text, or email** the petitioner? • **Send unwanted gifts** or other items to the petitioner? • **Monitor petitioner's phone calls**, computer use, or social media? • **Use technology**, like hidden cameras or global positioning systems (GPS), to track the petitioner? • **Drive by or hang out** at the petitioner's home, school, or work? • **Follow or show up** wherever the petitioner is?	Stalking increases risk of lethality. Stalking PL §120.45-60.
Petitioner's Belief	• Does the petitioner **believe that the respondent will re-assault or attempt to kill** the petitioner?	Petitioner's belief of harm is a lethality factor FCA §821(1).
Children	• Has there been **direct physical abuse? Threats to harm** children? Child **sexual abuse**? • Were **children present** during the incident? • Have the **children witnessed violence** between the parties? • Is the respondent the **biological** parent of the child(ren)?	Having a child who is not the respondent's increases lethality and recidivism. Assault during pregnancy increases risk of lethality. Children present increases risk of recidivism. FCA §842(b)(c) and following: court may limit custody or access on OP; court may include child as a protected party on OP, Annie C. v. Marcellus W., 278 AD2d 177 (1st Dept 2000).
Safety Planning	• **Are there safety measures in place**? Petitioner service referral? • Is the petitioner eligible for an attorney?	FCA §821-a requires court to inform both parties of right to attorney; §154-c(2) and §844 covers modification.

EVIDENCE FACT PATTERN:

Ramon, your client, lived with Tom for about 8 years. Ramon left Tom 10 months ago, and Tom will not accept that the relationship is over. Ramon is seeking an Order of Protection, because, as he tells you, "Things are just getting weirder and weirder," and he is feeling more and more threatened and scared by Tom's actions.

You want to try to prove a family offense, and will do that based on the evidence you have. The more pieces of evidence you can get admitted, the more likely that Ramon will end up with the OP he needs. (For this exercise, don't worry about the specific offense to prove. Just assume that you need to get the following evidence admitted in order to get the OP.) The pieces of evidence are:

1. Messages sent by Tom via Facebook messenger that Ramon says came from Tom, and which Ramon understands to be threats
2. Posts from Tom's Facebook page, which appear on Ramon's feed, and which make various disparaging comments about Ramon, Ramon's friends, and his family
3. Emails Ramon has received from Tom – some clearly threatening, and some that seem to be more innocuous, but that Ramon is frightened by
4. Thousands of text messages between the two, in some of which Tom states things like, "U will never get away" "We R meant to be 2gether" "ur boss is making u work 2 l8" "Why r u out dancing 2night?" "Whos the skank ur dancing wth, whore?" "hows ur dentist?" "hope U got good groceries might be hungry" "hope I don't have to teach U a lesson" "might not be so pretty after that" and Ramon keeps telling him, "Lv me alone!" "None of ur bizness who im with"
5. Several videos Ramon received of himself inside his apartment that seem to have been taken from outside his apartment, and which he believes Tom sent to show that he is watching Ramon
6. A photo of the area around Ramon's house, where he thinks Tom has been taking videos
7. A log Ramon has kept on his cell phone of all the times and places he saw, or "ran into" Tom in the past few months.
8. Ramon says he feels like Tom always knows where he is, and you find that there's GPS tracking software on the phone, disguised as a game program. Ramon says he didn't know that was there, but that Tom actually emailed him the game program a couple of months ago, when Ramon was still trying to remain friendly with Tom, so Ramon put it on his phone
9. Several photos Ramon took of Tom in places he didn't expect to see Tom

10. Dozens of calls Ramon has received where there was no one on the line, but Ramon feels like it was Tom. Some are from Tom's phone number, and some seem not to be
11. Voicemails Tom left on Ramon's phone – sometimes threatening, sometimes trying to win Ramon back
12. Cards from Tom Ramon has found stuffed under his door, and that say things about always being together, that Tom loves Ramon, that Tom hopes Ramon is feeling better (after a two-day period Ramon had been out of work with a cold)

- Messages through FB messenger that Ramon says came from Tom, and which Ramon understands to be threats

Q. Does Mr. Dirt have a FB account?

A. Yes

Q. How do you know this?

A. I have seen his fb page many times and I have received messages from him and been tagged by him.

Q. Under what name does he have a fb account?

A. Tom Dirt

Q. Do you have a FB account?

A. Yes

Q. Under what name?

A. Mine- Ramon Client

Q. Are you familiar with FB messenger?

A. Yes

Q. What is it?

A. It's a way to send private messages through FB, kind of like email

Q. Have you ever received correspondence from Mr. Dirt via FB messenger?

A. Yes

Q. When?

A. Many, many times.

Q. Directing your attention to April 23, 2016, did you receive any messages via FB messenger from Mr. Dirt?

A. Yes

I would like to have this marked as Petitioner's ex 10.

Q. Do you recognize P's ex 10?

A. Yes

Q. What is it?

A. messages sent to me by Tom on April 23, 2016

Q. When did you view this?

A. On April 23, 2016

Q. When did you print this out?

A. About 2 weeks ago.

Q. Is this a complete and accurate account of the message you received through FB messenger on April 23, 2016?

A. Yes

Your honor, I ask that P's ex 10 be admitted into evidence.

Q. Did there come a point when you asked Mr. Dirt to stop contacting you?

A. Yes

Q. When was that?

A. We broke up in October and I asked him to stop contacting me right before Christmas, on December 19.

Q. Did Mr. Dirt continue to contact you?

A. Yes. A ton.

Q. How would he contact you?

A. texts, calls, cards, posts on FB, FB Messenger. What ways didn't he contact me should be the questions.

OC: Objection, not responsive. Move to strike the last sentence.

Judge: Sustained, let the record reflect that last sentence is stricken.

Q. Directing your attention to FB Posts, did you continue to receive FB Posts after December 19, 2015?

A. Yes.

ADMIT FB POSTS

Q.Are you familiar with whether or not Mr. Dirt has a FB account?

A.Yes, he does.

Q. What name does he use on that account?

A. His name- Tom Dirt

Q. Do you have a FB Account?

A. Yes

Q. What name do you use on your FB account?

A. Mine- Ramon Client.

Your honor may I please have this marked as P's 8 for ID

Q.I am showing you Petitioner's exhibit 8, do you recognize this?

Yes

Q.What do you recognize this to be?

A.FB posts where Tom tagged me.

Q. Are these all the FB posts where you have been tagged by Mr. Dirt since December 19, 2015?

A. Yes

Q.Has it been altered in any way?

A.No

I ask that Petitioner's 8 be admitted into evidence.

OC- I object, we don't know how this exhibit was created or if it's been manipulated in any way.

Judge- Counselor, I agree with the fact that we don't know how it was created.

Q. Mr. Client, how was exhibit three created?

A. I did a search on FB account for all the times I was tagged by Tom in his FB posts since December 19, 2015.

Q. Does P's 8 accurately represent that search?

A. Yes

Q. Who printed this out?

A. I did

Your honor, I ask that Petitioner's 8 be admitted into evidence.

OC- I still object….

Judge: Petitioner's 8 admitted into evidence.

Q. When you say you were tagged in post, what do you mean?

A. When someone tags me in a post on their page, I receive a notification about the post.

Q. Mr. Client, can you please read the first post dated January 1, 2016?

A. 1st NY wo my guy Ramon

Q. Can you please read the second post from April 1, 2016?

A. IM ovr u Ramon AF

Q. can you please read the third post from May 28, 2016?

A. Ramon 2G2B4G 2EZ 2 Find

Q. Can you please the fourth post from June 18, 2016?

A. Ramon A picture with a quote inside, you have an innate ability to screw people over while making yourself look like the victim.

Q. Can you please read the fifth post from July 12, 2016?

A. It says ramon with another picture with a quote inside, the villain plays the victim so well.

Q. Can you please read the sixth from July 29, 2016?

A. hope I don't have to teach U a lesson Ramon u might not be so pretty after that

Q. Can you please read the seventh quote from August 7, 2016?

A. Whos the skank ur dancing wth, whore? Ramon

Q. Can you please read the eighth quote from August 9, 2016?

A. Ramon We R meant to be 2gether

Q. How did these messages make you feel?

A. They scared me because they got weirder and weirder. They made me feel like he was always watching me and he knew everything I was doing. At some points, I was afraid to leave my house because I didn't know if he would be there. I tried to be nice when I ended things, but he

just wouldn't stop.

- Emails Ramon has received from Tom – some clearly threatening, and some that seem to be more innocuous, but that Ramon is frightened by the emails

Q. Are you familiar with the email address of Mr. Dirt?

A. Yes.

Q. How are you familiar with it?

A. I have received many emails from him.

Q. What is his email address?

A. tommyd11@gmail.com

Your honor I would like to have this marked as Petitioner's exhibit 11.

Q. Do you recognize this?

A. Yes.

Q. What is it?

A. Emails I received from Tom.

Q. How many emails did you receive on June 4, 2016?

A. 7

Q. Do you recognize the email address?

A. Yes, it's Tom's email address.

Q. When did you receive these emails?

A. June 4, 2016

Q. When did you print these emails?

A. A couple of weeks ago.

Q. Do the emails appear to have been altered or changed in any way?

A. No

Q. Is this a complete and accurate account of the emails you received from Tom on June 4, 2016?

A. Yes

Q. Are all 7 emails contained in this exhibit?

A. Yes

Your honor, I ask that P's ex 11 be admitted into evidence.

- Thousands of text messages between the two, in some of which Tom states things like, "U will never get away" "We R meant to be 2gether" "ur boss is making u work 2 l8" "Why r u out dancing 2night?" "Whos the skank ur dancing wth, whore?" "hows ur dentist?" "hope U got good groceries might be hungry" "hope I don't have to teach U a lesson" "might not be so pretty after that" and Ramon keeps telling him, "Lv me alone!" "None of ur bizness who im with"

Q. Are you familiar with the cell phone number of Mr. Dirt?

A. Yes

Q. What is it?

A. 914-555-1212

Q. Have you received calls and texts from him before?

A. Yes

I would like to have this marked as Petitioner's exhibit 1 for identification

Q. Do you recognize this?

A. Yes

Q. What is it?

A. These are texts sent to me by Tom

Q. How do you know they were from Mr. Dirt?

A. That's his number

Q. When did you receive these series of texts?

A. November 4-5, 2015.

Q. When did you print out these texts?

A. A couple of weeks ago.

Q. Do the texts look the same as they did Nov 4-5 2015?

A. Yes

Q. Have they been changed in any way?

A. No

Q. Is this a complete account of all the texts between you and Mr. Dirt on Nov 4-5, 2015?

A. Yes.

I ask that Petitioner's Ex 1be admitted into evidence.

- Several videos Ramon received of himself inside his apartment that seem to have been taken from outside his apartment, and which he believes Tom sent to show that he is watching Ramon

Q. Mr. Client, did you receive a video of you via email on March 17, 2016?

A. Yes

Q. From whom?

A. the email address was icuramon@gmail.com.

Q. Did you recognize this email address?

A. No, I had never received an email from that person before.

Q. What, if anything, was in the email?

A. There was an attachment for a video in the email

Q. What was the video?

A. It was a video taken of me inside my apartment.

You- Your honor, at this point I would like to show the video marked as P's ex 6 and have it marked for identification. I have already provided a copy to opposing counsel.

OC- Objection, it is not in evidence and we do not know who took the video.

You- I have to lay the proper foundation in order to admit it and part of that is viewing the videotape.

Judge- please show the video

After video

Q. Is that the same video you received on March 17, 2016?

A. Yes

Q. Has it been altered in any way?

A. No

Q. What does the video show?

A. It's me in my home.

Q. Do you know who took the video?

A. No

Q. Do you know when the video was taken?

A. Sometime since October 2015 because that is when I moved into this house.

Your honor, I ask that this video be admitted into evidence as P's ex 6.

OC: I object. We don't know who took the video or when it was taken.

You: We have admitted we don't know who took the video, but we do know it was taken after October 2015. Opposing Counsel's arguments go to the weight of the evidence, not admissibility.

- A photo of the area around Ramon's house, where he thinks Tom has been taking videos

Your honor I would like to have this photograph marked as P's ex 7 for identification

Q. Mr. Client, do you recognize this photo?

A. Yes.

Q. What is it?

A. An area outside of my house, near one of my windows.

Q. Are you familiar with this area?

A. Yes.

Q. Does it fairly and accurately represent that area?

A. Yes

Q. Does it fairly and accurately represent the area as it appeared on March 17, 2016?

A. Yes.

Your honor, I ask that P's ex 7 be admitted into evidence.

- A log Ramon has kept on his cell phone of all the times and places he saw, or "ran into" Tom in the past few months.

Q. When, if ever, did you see Mr. Dirt while out running errands or just out of your home?

A. I saw him any times at place where I didn't expect to see him.

Q. How did this make you feel?

A. Nervous and scared. I didn't know why he was there.

Q. What did you start doing when you noticed that you were seeing him?

A. I started keeping a log on the notes section of my iPhone.

Q. When you say a log what do you mean?

A. I opened up the notes app on my phone and wrote down when and where I saw him in a document I entitled seeing tom.

Q. When did you start this log?

A. On February 3, 2016 when I saw him at my new gym, not the one I went to when Tom and I were together.

Q. Why did you start this log?

A. I wanted to make sure I remembered when I saw him and to see if there was a pattern I could try to figure out.

I would like this marked as Petitioner's ex 15 and please hand it to the witness.

Q. Do you recognize this exhibit?

A. Yes.

Q. What is it?

A. It's the log I kept on my phone every time I saw Tom and I had my phone with me after Feb 3, 2016

B. Q. Were there times that you saw him that aren't in this log?

A. Yes.

Q. Have you reviewed this log?

A. Yes

Q. Does it appear to have been altered in any way?

A. No

Q. Who printed out this log?

A. I did.

Q. When?

A. a couple of weeks ago.

I ask that this be admitted into evidence as Petitioner's 15.

OC- objection. There is no reason that Mr. Client can't just testify about when he says he saw my client and this was prepared in anticipation of litigation.

- Ramon says he feels like Tom always knows where he is, and you find that there's GPS tracking software on the phone, disguised as a game program. Ramon says he didn't know that was there, but that Tom actually emailed him the game program a couple of months ago, when Ramon was still trying to remain friendly with Tom, so Ramon put it on his phone.

Q. Directing your attention to October 23, 2016, do you remember if you received an email from Mr. Dirt?

A. Yes

Q. What did the email say?

OC- Objection, hearsay.

Your Honor, this is a statement of a party opponent.

Judge- overruled, please answer the question

A. That he had a game he thought I would like and he included a link to the game. Tom knows I really like to play different games on my phone.

Q. What, if anything, did you do with the link to the game?

A. I downloaded it to my phone.

Q. Did you reply to the email?

A. Yes, I said thanks. I was still trying to be friendly at this point.

Q. Are you familiar with Mr. Dirt's email address?

A. Yes.

Q. How are you familiar with Mr. Dirt's email address?

A. I've received a lot of emails from him and I sent him a lot of emails before we broke up.

Q. What is his email address?

A. tommyd11@gmail.com

Your Honor, may I please have this marked as exhibit 2 for identification and given to the witness?

Q. Do you recognize this exhibit?

A. Yes

Q. What is it?

A. It's a copy of the email that I received from Tom on October 23, 2015 and my response.

Q. How do you know it's from Mr. Dirt?

A. Because the email address is tommyd11@gmail.com.

Q. When did you receive this email?

A. October 23, 2015.

Q. When was the email printed?

A. A couple of weeks ago.

Q. Does the email look the same as when you saw it on October 23, 2015?

A. Yes.

Q. Has it been altered in any way?

A. No

Your honor I ask that Petitioner's 2 be admitted into evidence.

Judge- admitted as Petitioner's 2.

Q. You said earlier that you downloaded the link to your phone?

OC- Objection, asked and answered

Your Honor, I am just transitioning subjects.

Judge- we know he downloaded the game, objection sustained. Please move on, Counselor.

Q. After you downloaded the game, what, if anything, did you notice?

A. It was really weird, all of a sudden Tom was everywhere that I was. I would go out to a bar and he would be there about 5 minutes after me.

Q. Were these bars you went to with Mr. Dirt?

OC- Objection, leading.

Your Honor, it's not a leading question because the witness can say yes or no or sometimes.

Overruled. Please answer the question.

A. No, I started going to new places when Tom and I broke up.

Q. When, if ever, were there other times you saw him?

A. It seemed like everywhere for a while, he always showed up about 5-15 minutes after I did- the movies, the grocery store, the gym, restaurants.

Q. Were these places you usually went to with Mr. Dirt?

A. Not all of them- I changed gyms and started going to to different restaurants because I moved. We sometimes went to the movie theater.

Q. What, if anything, did you do once you noticed you started running into Tom at different places?

A. I took my iphone to the local apple store.

Q. Why?

A. I wanted to see if the game I downloaded had something in it that could track where I was.

Q. Without telling us what they said, did you get an answer from the Apple store?

A. Yes.

Your honor I would like to ask that this subpoena, this disc and corresponding certification and this print out of these records from Apple be marked as Petitioner's exhibit 3, 4 and 5.

I am showing these exhibits to opposing counsel.

Your honor I offer these records into evidence under CPLR 3122-a and 4518. As you can see from the accompanying certification the records from Apple were made in the regular course of business and it was the regular course of this business to make these records. The records were made at the time of the act or a reasonable time thereafter. Under these rules, the certification stands as a foundation for these records.

OC- Objection, I was not given 30 days notice as required under CPLR 3122a.

You- Your honor I repeatedly requested these records from the Opposing party in my conversations with Opposing Counsel on August 30, 2016 and September 2, 2016. I also informed him of my intention to use these records at trial on September 2, 2016. Finally, after your honor signed the subpoena, I served a copy on opposing counsel. In addition, I made him aware when the disk was available at the court and when company offered me a linked access to the records because I did not have the right software to view them, I promptly shared that with OC. Therefore the OC cannot complain that I did not notify him of my intention to use these records at trial. Assuming arguendo that the court finds that I did not notify him properly, the mere fact that an objection has been raised should not preclude the use of the certification procedure to satisfy CPLR 4518. This is a proper certification of business records and they should be admitted.

Judge- overruled, these records are admitted.

- Several photos Ramon took of Tom in places he didn't expect to see Tom

Q. You have mentioned seeing Mr. Dirt in places where you didn't expect to see him, what, if anything did you do?

A. I started to take pictures of him with my iPhone.

Q. When did you start doing this?

A. The first one was when I saw him for the third time at my new gym on December 4, 2016.

Your honor I would like to have this marked as Petitioner's exhibit 9 for identification and given to Mr. Client.

Judge: so marked

Q. I am showing you what has been marked as Exhibit 9 for identification. Do you recognize what is shown in this photograph?

A. Yes, it's the picture I took of Tom at my gym on December 4, 2015.

Q. Does the scene portrayed in the photograph fairly and accurately represent the scene as you remember it on December 4, 2015?

A. Yes

Q. Has it been altered in any way?

A. No.

Your Honor, I move Petitioner's 9 into evidence.

- Dozens of calls Ramon has received where there was no one on the line, but Ramon feels like it was Tom. Some are from Tom's phone number, and some seem not to be

Q. Did there come a point when you began receiving calls where the person on the line said nothing?

A. Yes.

Q. When did this start occurring?

A. In November.

Q. How long did it continue?

A. Through August 2016

Q. Have you received telephone calls from Mr. Dirt?

A. Yes

Q. What is his number?

A. 914-555-1212

Q. When you received some of these calls, what, if anything, did Mr. Dirt say?

A. Nothing, it was just dead air.

Q. Did you receive any other similar calls?

A. Yes

Q. From what number?

A. I don't know, it said unknown.

Your honor, I would like to have this marked as Petitioner's ex 17 for identification. I am providing a copy to opposing counsel. After marked I would like it handed to the witness.

Q. Mr. Client, do you recognize this?

A. Yes

Q. What is it?

A. It's a print out of my cell phone bills from November 2015 through August 2016.

Q. What does it show?

A. All the calls where the caller was silent.

Q. Has it been altered in any way?

A. I blacked out all the calls that were not the calls where the caller remained silent.

Q. Does this accurately reflect all the calls you received where the caller was silent?

A. Yes

Your Honor, I ask that Petitioner's 17 be admitted into evidence.

OC: Objection, this has been altered and isn't an unaltered print out of the records and they aren't certified. In addition, we don't know who called from the unknown number.

You: Your Honor, these records reflect exactly what my client testified to, calls from Mr. Dirt's phone where the caller remained silent and calls from an unknown number where the caller remained silent. This exhibit saves the court time from hearing about each and every call because the exhibit shows the calls and my client testified that he is the one who blacked out the other calls. As to not knowing to whom the unknown number belongs that goes to weight of the evidence not admissibility.

- Voicemails Tom left on Ramon's phone – sometimes threatening, sometimes trying to win Ramon back

Q. When, if ever, did Mr. Dirt call you after you ended the relationship?

A. Many times.

Q. When, if ever, did he leave you voicemails?

A. Many times.

Q. Have you spoken with Mr. Dirt before?

A. Yes

Q. Have you received telephone calls from Mr. Dirt before?

A. Yes

Q. On what dates did you receive voicemails from Mr. Dirt?

A. I'm not sure of the exact dates because there were quite a few.

Q. Is there anything that would refresh your recollection?

A. Yes, my timeline.

Your Honor, if I may have the court officer hand my client his time-line

OC- I must be shown this right now, I haven't seen it.

Your Honor, I am not asking that this be admitted into evidence, I am requesting that my client be able to review it. Opposing counsel does not have the right per case law to review it right now.

Judge- please hand the timeline to the witness.

You- Mr. Client, please review the document and if it refreshes your memory, please place it face down and look up.

Q. Do you now remember the dates of the voicemails?

A. Yes- January 16, January 28, February 14, February 28, March 18, April 19, May 13, May 28, May 31, June 2, June 6, June 19, July 4, July 26, August 9, August 18, and August 30, 2016.

Your Honor, I ask that this disk be marked as exhibit 24 for identification. I have already provided opposing counsel with a copy of the disk.

Q. Have you heard the recordings on exhibit 24?

A. Yes.

Q. What is the recording?

A. They are the voicemails from the dates I already mentioned.

Q. How was the disk created?

A. I copied all of the saved voicemails on to the disk.

Q. Are the recordings contained on exhibit 24 complete recordings of the voice mails on the mentioned dates?

A. Yes.

Q. Have they been altered in any way?

A. No.

Q. Are the voice mails all left my the same person?

A. Yes.

Q. Do you recognize the voice?

A. Yes

Q. To whom does it belong?

A. Tom.

Your Honor, I ask that Petitioner's 24 be admitted into evidence.

OC- Objection, we don't know that these calls haven't been manipulated or changed and this isn't best evidence because it's not coming from the actual phone on which the messages were left.

You- Your Honor, my client testified that these are complete recordings and it will be up to your Honor to determine credibility, but that goes to weight, not admissibility. In addition, courts have routinely allowed copies of voicemails to come in as evidence. To require my client to give his cell phone to the court during the totality of this trial and any potential appeal is unduly burdensome.

- Cards from Tom Ramon has found stuffed under his door, and that say things about always being together, that Tom loves Ramon, that Tom hopes Ramon is feeling better (after a two-day period Ramon had been out of work with a cold)

Q. Did there come a point when you began receiving cards from Mr. Dirt?

A. Yes

Q. When was that?

A. It started in November 2015 and continued periodically through May 2016.

Q. How do you know the cards were from Mr. Dirt?

A. They were signed by him.

Q. Have you seen his signature and handwriting before you began receiving these cards in November 2015?

A. Yes, many times.

Q. What did the first card say in November 2015?

A. That he loves me, we should always be together and I can't get away from him.

I would like this marked as Petitioner's exhibit 12 for identification and then please hand it to the witness.

Q. Mr. Client, do you recognize this?

A. Yes

Q. What is it?

A. It's a card from Tom that I found stuffed under my door in November 2015?

Q. What does the card say?

A. That Tom loves me, we should always be together and I can't get away from him.

Q. How do you know it's from Mr. Dirt?

A. I recognize his handwriting.

Q. Is this card in the same condition as when you received it in November 2015?

A. Yes

Q. Has it been changed in any way?

A. No

Your honor I ask that P's 12 be admitted into evidence.