

# practical (and understandable) ways to protect yourself and your clients from 21st century headaches

Kenneth G. Raggio  
Dallas, TX

J. Benjamin Stevens  
Spartanburg, SC


Susan Saper Galamba  
Overland Park, KS

Todd M. Frankfort  
Houston, TX





## The Man With No Secrets—at All

Security level: 1 

**Profile:** You're a digital exhibitionist—and an identity thief's perfect target.

**Digital tech:** One password to rule them all (last four of your Social Security number should do it); unsecured Wi-Fi; phone Password Lock set to Off.

**Social networks:** Facebook, Snapchat, Pinterest, Twitter, Instagram—you name it. Privacy settings? What are those?

**Commerce:** The more retail loyalty programs you can join, the better you like it.

## You Floss Nightly—and Clear Your Web Cache

Security level: 2  


**Profile:** Sure, you know the NSA and Target are both listening in. Creepy? Sort of. You'll take precautions—but you're not giving up Scramble With Friends just to make a point.

**Digital tech:** For Web browsing, privacy add-ons (e.g., HTTPS Everywhere, Disconnect); for email, two-step verification and strong passwords; WPA-encrypted Wi-Fi.

**Social networks:** All networks, but with strong privacy settings and a password manager.

**Commerce:** Amazon Prime, baby . . . You can't give up everything.

## Paranoid? No, Realistic

Security level: 3   





**Profile:** They laughed at your talk of government surveillance, but that was before Edward Snowden. Who's paranoid now?

**Digital tech:** VPN (virtual private network), OTR (Off The Record) instant messaging for laptops, and Silent Circle for mobile phone calls; PGP (Pretty Good Privacy) email encryption.

**Social networks:** Offline only—you meet your buddies at the Def Con Hacking Conference.

**Commerce:** No loyalty cards; you give "Jenny's Number" (XXX-867-5309) to store clerks to look up "your" account.

## Welcome To the Encrypted Zone

Security level: 4    






**Profile:** You're a CIA agent or democracy activist in a totalitarian state. Or maybe you just think like one. Welcome to the privacy rabbit hole.

**Digital tech:** Air-gapped computers (meaning no Web connection) for sensitive files; burner phones; the Tor bundle with VPN. Open-source technology.

**Social networks:** Offline only. Immediate family, trusted members of your doomsday-prepper network.

**Commerce:** Cash, barter in MREs . . . or bitcoins.

## Living Off the Grid, Under A Rock

Security level: 5     

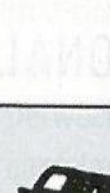
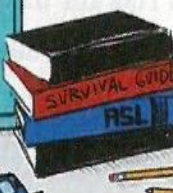
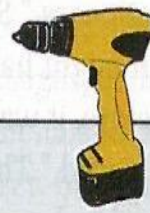
**Profile:** You don't want to worry about digital snooping—ever. So you've gone offline.

**Digital tech:** Does finger painting count? Absolutely no computers.

**Social network:** Other woodland creatures, your reclusive aunt.

**Commerce:** Cash, foraging for edible roots.

trum? Side with  
never have to  
ne from spam-  
th you. Join the  
ements, and  
l be happiest  
digital dweller.







# List of Concerns...

Email

Encryption

Forensic Backups

Social Media

Sniffers

Spoliation

Cloud Computing

Data Mining

Litigation Holds

Recording  
(video & audio)

Hacking

Keystroke Loggers

Thumbcams

Disappearing Texts

Remote Access

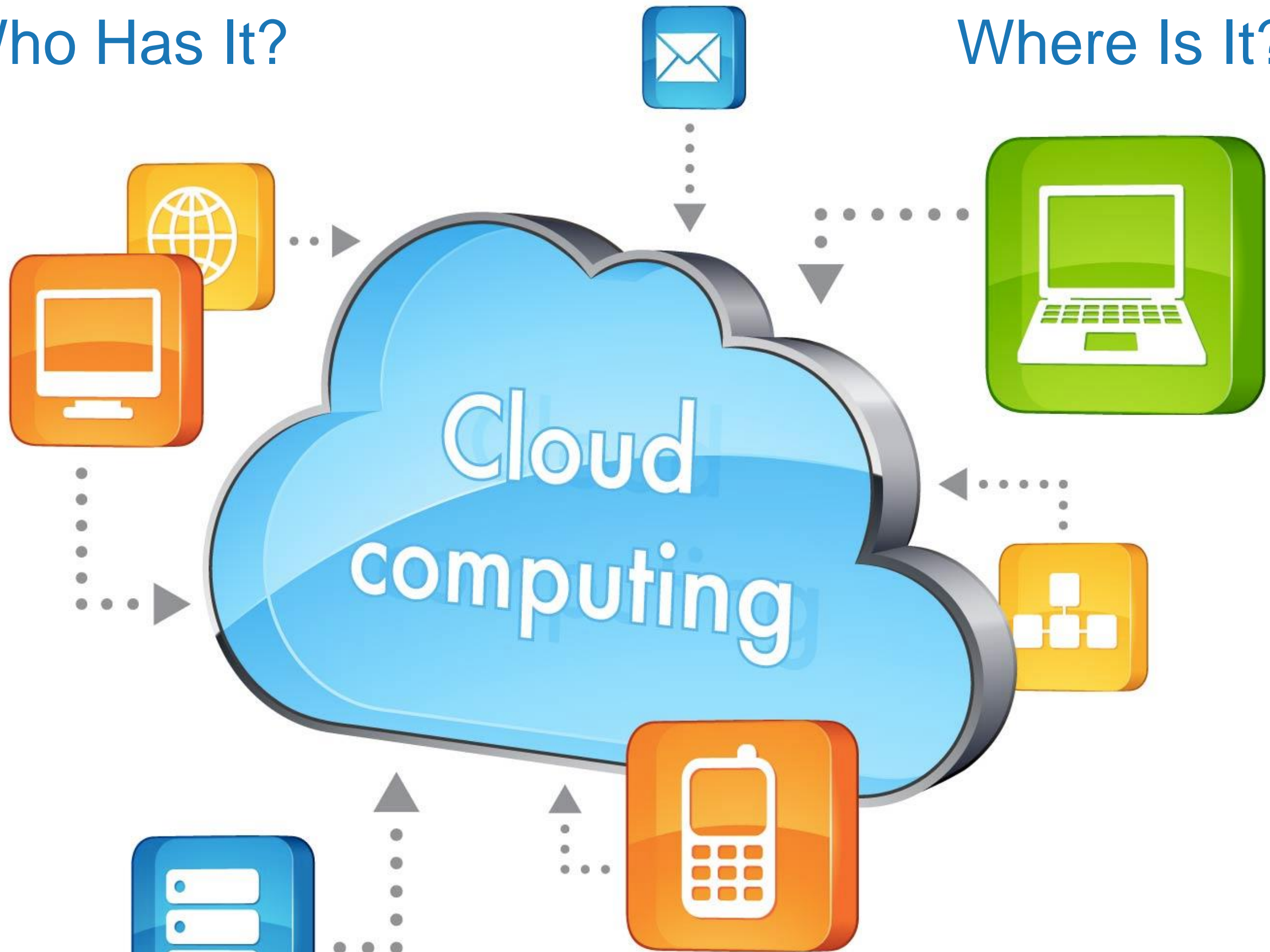
Leaving Devices On

Malware

Call Spoofing

Who Has It?

Where Is It?



Read?

Retrievable?



# Model Rule 1.1 Comment 8

AMERICAN BAR ASSOCIATION

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject



Competent representation includes knowledge of social media and an understanding of how it will impact the client's case including the client's credibility.

If a client's postings on social media might impact the client's legal matter, the lawyer must advise the client of the legal ramifications of existing postings, future postings, and third party comments. Advice should be given before and after the law suit is filed



# California ESI

A fundamental duty of an attorney is '[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client...

...duty to assert the attorney-client privilege to protect confidential communications between the attorney and client which are sought in discovery...

...privileged information, of a client remain confidential and that the attorney's handling of a client's information does not result in a waiver of any confidence, privilege, or protection, is a fundamental part of an attorney's duty of competence.





# Texas Disciplinary Rule 1.05

...shall not knowingly “reveal confidential information...”

Confidential information includes both privileged information and unprivileged client information

Unprivileged client information means all information relating to a client...



nelson / simek security basics: 12  
Have a strong password (at least 12 characters)

*A strong 12-character password  $\pm$  17 years to crack*

Don't use the same password everywhere

Change your passwords regularly

Do not have a file named "passwords" on your computer

Change the defaults

nelson / simek security basics:

Laptops should be protected with whole disk encryption – no exceptions.

Backup media should be encrypted (if online, both in transit and while stored).

Thumb drives should be encrypted.

Make sure you have a PIN for your phone.

Don't use "swiping" to protect your phone

# nelson / simek security basics:

Make sure that you can wipe your data remotely if you lose your phone.

Use a single integrated product to deal with spam, viruses, and malware.

Encrypt Wireless networks – WPA or WPA2

Apply/install all critical software patches



# nelson / simek security basics:

Don't use an XP computer or other unsupported software

Control Access

Cloud: understand your provider contract

Watch permissions requested by social media

Cyber insurance?

# nelson / simek security basics:

Dispose of your data receptacles  
**SECURELY**

- Digital copier
- Computers
- Thumb drives/SD cards
- Low tech: SHRED!

Use wireless networks with great care

Use a VPN or other encrypted connection  
for remote access

1.393

72%

facebook.

890

157



## We're updating our terms and policies and introducing Privacy Basics

Facebook <notification+m55m5gmx@facebookmail.com>

Sent: Mon 11/24/2014 11:05 AM

To: Ken Raggio



Hi Ken,

We wanted to let you know we're updating our terms and policies on January 1, 2015 and introducing Privacy Basics. You can check out the details below or [on Facebook](#).



**facebook**  
*Privacy*

Over the past year, we've introduced new features and controls to help you get more out of Facebook, and listened to people who have asked us to better explain how we get and use information.

Now, with [Privacy Basics](#), you'll get tips and a how-to guide for taking charge of your experience on Facebook. We're also updating our [terms](#), [data policy](#) and [cookies policy](#) to reflect new features we've been working on and to make them easy to understand. And we're continuing to [improve ads](#) based on the apps and sites you use off Facebook and expanding your control over the ads you see.





271

500

23%





**WhatsApp**



*Instagram*





YOU HAVE BEEN  
HACKED !



## Hacking Airlines, Ships, and More Through Satellite Communications

Aug 08, 2014 2:10 PM EST | [3 Comments](#)

By [Max Eddy](#)



During one of the most anticipated Black Hat presentations, IOActive's Ruben Santamarta demonstrated the numerous flaws he discovered in satellite communication systems. Why should you care about Satcom? If



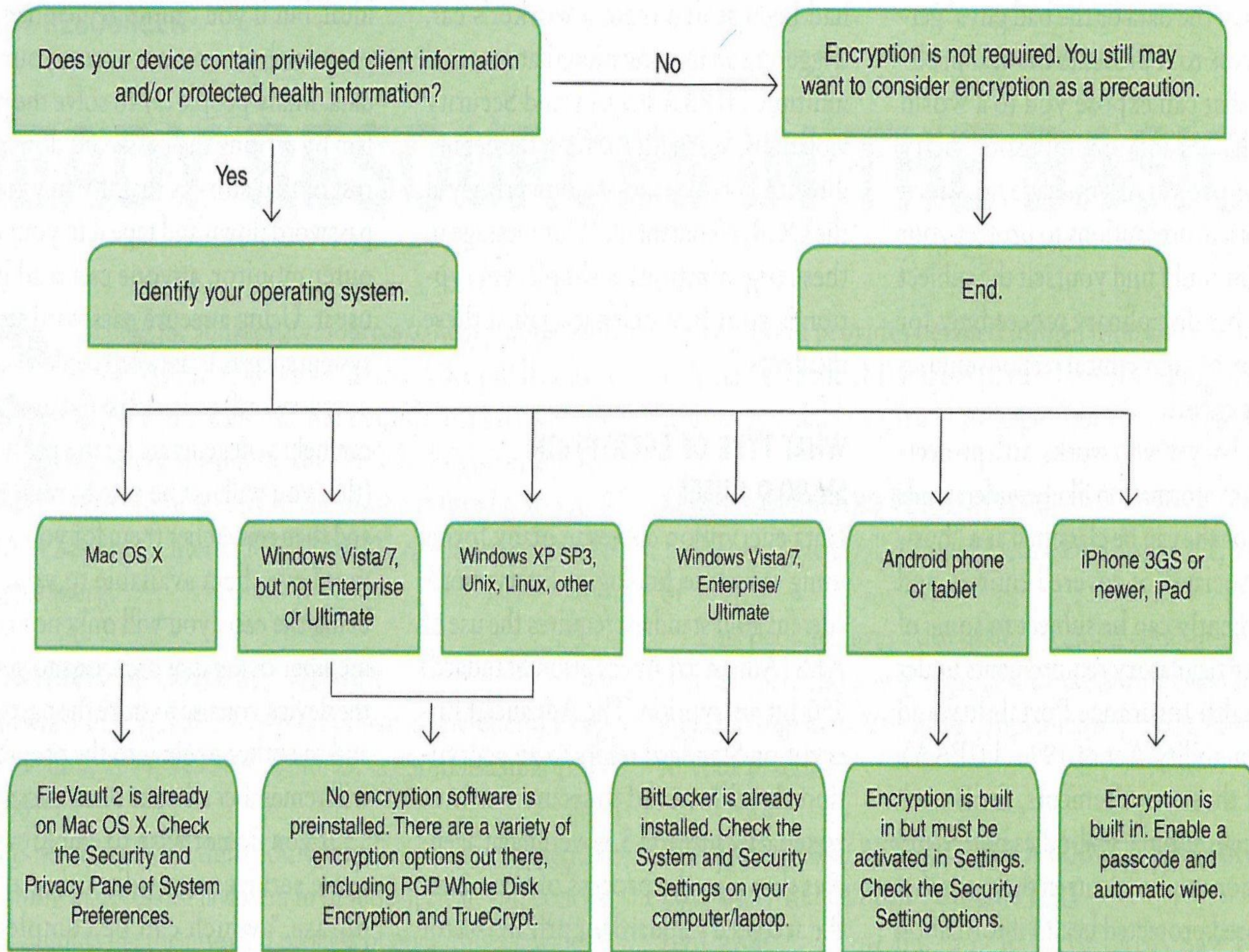
# P@\$\$W0RDS





# ENCRYPTION









AMERICAN ACADEMY  
**AAML**<sup>TM</sup>  
OF MATRIMONIAL LAWYERS  
**WEBINARS**

# "For Your Eyes Only" Confidential Information and The Ethics of Technology in the Law Office

FERGUSON CASE ORR PATERSON LLP  
ATTORNEYS AT LAW  
1050 SOUTH KIMBALL ROAD, VENTURA, CALIFORNIA 93004  
PHONE: (805) 659-8800 FAX: (805) 659-8810  
WWW.FERGUSONCLO.COM

MICHAEL W. CASE  
JOHN C. BIRN  
THOMAS J. ENGLISH  
JOSEPH L. FERGUSON, JR.  
DAVID H. FERGUSON  
HENRY C. LACHNER  
 DAVID L. BAKER  
DEPT. D. BAKER  
WILLIAM D. BAKER  
CHRISTOPHER A. BAKER  
DAVID H. BAKER  
DAVID D. BAKER  
 JAMES S. HENDERSON  
NANA T. HENDERSON  
MICHAEL A. HENDERSON  
DOUGLAS P. HENDERSON  
JAMES S. HENDERSON  
LESLIE A. HENDERSON  
 DEPT. D. HENDERSON  
JOHN M. HENDERSON  
NANA T. HENDERSON  
JOHN A. HENDERSON  
JENNIFER A. HENDERSON  
KATHLEEN E. HENDERSON  
 LAUREN E. HENDERSON  
ERIC A. HENDERSON  
LAUREN E. HENDERSON  
ANNA L. HENDERSON  
LARA J. HENDERSON  
 THOMAS S. FERGUSON  
DEPT. D.  
WILLIAM S. FERGUSON  
DAVID H. FERGUSON  
ROBERT S. ENGLISH

TO: CLIENT  
FROM: GREGORY W. HERRING

**PERSONAL INFORMATION AND PRIVACY, AND RELATED CONCERNS**

**Personal Information and Privacy:**

Our ability to represent you depends on your providing us with complete and truthful information. We rely upon the full and complete truthfulness of the information you provide to us in formulating strategy, giving you advice and calculating the best positions to be taken. Your failure to provide us with full and complete truthful information, or withholding from us any negative information, could materially adversely affect the outcome of your case. Our ability to provide the best service on your behalf requires your continued cooperation in this regard and that you be prompt in responding to our questions and requests for information.

During the course of our representation, we will need to collect sensitive data including without limitation your personal financial information. We are committed to protecting this information.

We completely understand the need to safeguard sensitive information about you and we maintain standards and procedures designed to prevent misuse. We collect information about you only to help us protect you and your interests.

Please understand, however, that sensitive information that is required to be disclosed to the other party in litigation, or filed with the court, may then be used by anyone who comes into its possession. Please also be very clear that the content of all court filings is most probably going to be available for examination by the public, as court files are very rarely sealed.

Generally speaking, eavesdropping and recording private communications by another person is illegal. Additionally, such evidence would be inadmissible under the Family Code. I believe that these principles could reasonably be extended to the reading of private email messages and copying of electronic data.

Serious problems can also arise with other forms of surveillance, such as hidden cameras, automobile tracking and etc.

WESTLAKE VILLAGE OFFICE  
4000 TOWNSHIRE ROAD, SUITE 200, WESTLAKE VILLAGE, CALIFORNIA 91391  
PHONE: (818) 899-8800 FAX: (818) 899-8810

**GORDON D. CRUSE**  
A PROFESSIONAL LAW CORPORATION

CERTIFIED SPECIALIST - FAMILY LAW  
BOARD OF SPECIALIZATION  
STATE BAR OF CALIFORNIA

402 West Broadway  
Suite 1210  
SAN DIEGO, CALIFORNIA 92101-8518  
TELEPHONE: (619) 496-9922  
FAX: (619) 496-0586

**INFORMATION REGARDING  
SOCIAL NETWORKING AND ELECTRONICS**

Because the Internet could be a source of much public information about yourself, I need to know what presence, if any, you have there. Just "Googling" a name often provides valuable information and is permissible. To properly advise you, I need to know the following:

- Do you have a profile on a social network like Facebook, Twitter, Linked-in, MySpace, Google Plus, etc.? \_\_\_\_\_
  - Is it in your name? \_\_\_\_\_
  - How many such profiles do you have? \_\_\_\_\_
  - Are they open to the public? \_\_\_\_\_
  - What is posted? \_\_\_\_\_
  - When was your most recent change to your social media site? \_\_\_\_\_
  - Where else do you post your communications? \_\_\_\_\_
  - Have you commented on articles, blogs, or pictures on other people's social media sites? \_\_\_\_\_
- Do you have your own website? \_\_\_\_\_
  - If so, what is the site(s) name? \_\_\_\_\_
  - How long have you had it? \_\_\_\_\_
  - When did you first launch the site? \_\_\_\_\_
  - When was your site last changed? \_\_\_\_\_
- Do you have a blog? \_\_\_\_\_ If so, what is the name? \_\_\_\_\_

RAGGIO & RAGGIO, PLLC

RAGGIO FAMILY LAW



**INFORMATION REGARDING  
SOCIAL NETWORKING AND ELECTRONICS**

Because the Internet could be a source of much public information about yourself, we need to know what presence, if any, you have there. Just "Googling" a name often provides valuable information and is permissible.

Also, all of us now have much reliance upon, and information contained in, electronic devices such as computers, tablets, cell phones, and digital cameras. To properly advise you, we need to know the following:

- Do you have a profile on a social network like Facebook, Twitter, Linked-in, MySpace, Google Plus, etc.? [Y] [N]
  - Is it in your name? [Y] [N]
  - If not in your name, what is the name associated with the profile? \_\_\_\_\_
  - How many such profiles do you have? \_\_\_\_\_
  - Are they open to the public? [Y] [N]
  - What is posted? \_\_\_\_\_
  - When was your most recent deletion or change to each of your social media sites? \_\_\_\_\_
  - Where else do you post your communications? \_\_\_\_\_
  - Have you commented on articles, blogs, or pictures on other people's social media sites? [Y] [N]
  - Do you use social media software (such as X1 Social Discovery software or Archive Social software) that collects and makes a record of all entries and data (or "mines" everything) that is currently on or has been on your social media site, or would do the same on someone else's social media site? [Y] [N]
- Do you have your own website? [Y] [N]
  - If so, what is the site(s) name? \_\_\_\_\_
  - How long have you had it? \_\_\_\_\_
  - When did you first launch the site? \_\_\_\_\_
  - When was your site last changed? \_\_\_\_\_
- Do you have a blog? [Y] [N]
  - If so, what is the name? \_\_\_\_\_
  - What do you post there? \_\_\_\_\_

3318 OAK GROVE AVENUE, DALLAS, TEXAS 75204 | 214 880-7500 | FAX 214 880-7508 | WWW.RAGGIOLAW.COM | KENNETH@RAGGIOLAW.COM

# Short Client Consent

Electronic mail is the Firm's preferred means of communication and is often more responsive to the client's needs, but may be less secure. Client ☐ does or ☐ does not wish to communicate with Attorney via e-mail, given the risks of inadvertent disclosure of privileged information.



# Long Client Consent

ORRIS H. RAGGIO (1988)  
LOUISE B. RAGGIO (2011)  
THOMAS L. RAGGIO\*  
KENNETH G. RAGGIO\*  
ORRIS H. RAGGIO, JR.\*  
BARBARA G. VAN DUYN  
JEFFREY T. RAGGIO (2014)

Law Offices of  
**RAGGIO & RAGGIO, P.L.L.C.**

3316 OAK GROVE AVENUE  
DALLAS, TEXAS 75204  
214/880-7500

FAX: 214/880-7506  
Website: <http://www.raggiolaw.com>

FELLOW  
AMERICAN ACADEMY OF  
MATRIMONIAL LAWYERS

\*CERTIFIED SPECIALISTS  
FAMILY LAW  
TEXAS BOARD OF  
LEGAL SPECIALIZATION

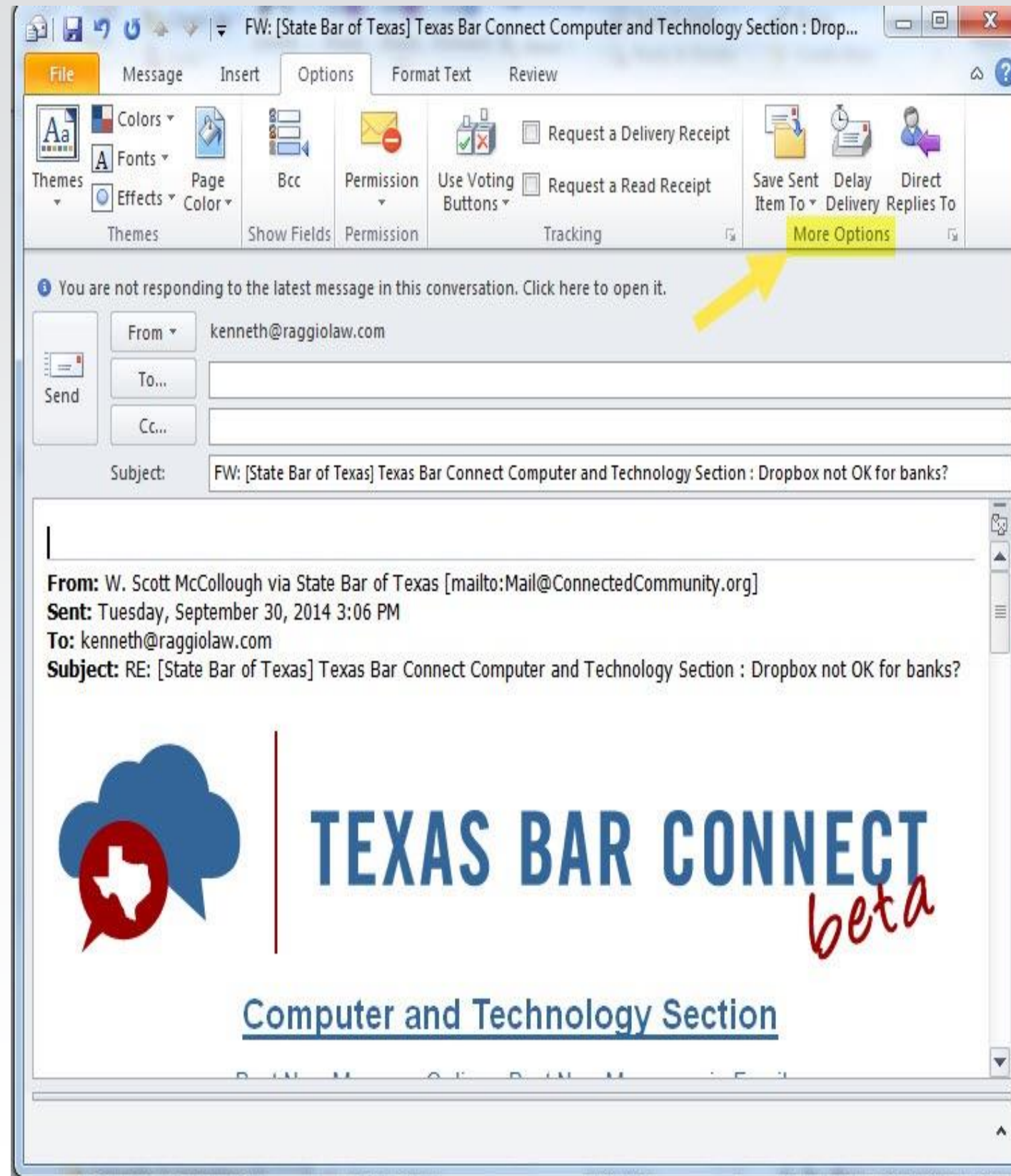
## E-MAIL COMMUNICATION

As you are undoubtedly aware, there is a danger of unintended disclosure of confidential client information when you communicate with us or we communicate with you via e-mail as a result of inadvertent dissemination of e-mails. Thus, our office has developed a policy regarding e-mails, and it is set forth below. After you read the policy, we ask that you check the appropriate box at the end of this letter, sign the acknowledgment and return it to our office.

The e-mail policy of the firm is:

1. No one can guarantee the security of e-mail communications. We do not employ encryption methods. Any use of e-mail is at your own risk.
2. Do not send an e-mail from an address where you do not want a reply to be sent. We assume that, if we receive an e-mail communication from you, it is safe to send a reply message back to that address.

# Encrypt in Outlook







## Properties

### Settings



Importance:

Normal

Sensitivity:

Normal

☐ Do not AutoArchive this item

### Voting and Tracking options



☐ Use voting buttons:

☐ Request a delivery receipt for this message

☐ Request a read receipt for this message

### Delivery options

### Security



Change security settings for this message.

Security Settings...

om: W.  
nt: Tue



## Properties

### Security Properties

- ☒ Encrypt message contents and attachments
- ☐ Add digital signature to this message
  - ☐ Send this message as clear text signed
  - ☐ Request S/MIME receipt for this message

Security Settings

Security setting:

<Automatic>

Change Settings...



## Welcome to E-mail Security

You have performed an action which uses the cryptographic e-mail features of Outlook. However, in order to use cryptographic e-mail you need a valid digital ID on your computer.

### What is a Digital ID?

A digital ID gives you the ability to digitally sign messages and prove your identity to those you communicate with. Additionally, you can encrypt (scramble) your messages so that they can be read only by their intended recipients.



By clicking the 'Get Digital ID' button below, you can get a digital ID from either an external Certification Authority (for internet e-mail), or from your Exchange Server administrator.

☒ Do not show this dialog again

Get Digital ID...

OK

// Digital Certificates

## Setting Up Outlook 2010 to Use Signing and Encryption Certificates

- Operating System: Windows XP, Windows Vista, Windows 7
  - Application: Outlook 2010
1. Make sure that you have [imported your certificates into the Windows Certificate store](#).
  2. Open Outlook.
  3. From the **File** menu, click the **Options** menu, select the **Trust Center** section and click the **Trust Center Settings** button.
  4. Click **E-mail Security** section.
  5. Select the following options:
    - **Add Digital Signature to Outgoing Messages**. This option includes your signing certificate on all outgoing messages.

# Another Option: Virtru

SEND

SECURE

EMAILS

When composing, turn ON  
Virtru to encrypt your email.  
Hit Send Secure when you are  
done.



NEXT



# Recipients simply verify their identity to unlock and read

Virtru is as easy for recipients as it is for senders. They can read your message anywhere, without installing any software. As soon as they verify their identity, they'll be able to read your messages and files.





# SET SECURITY OPTIONS

Virtru gives you additional security options for greater control.



NEXT





# ADJUST SECURITY OPTIONS

After you've sent your email,  
adjust your security options,  
including forwarding and  
expiration.



NEXT



# REVOKE YOUR EMAIL

Want to take it back? Just find your message in your sent items folder and click revoke.



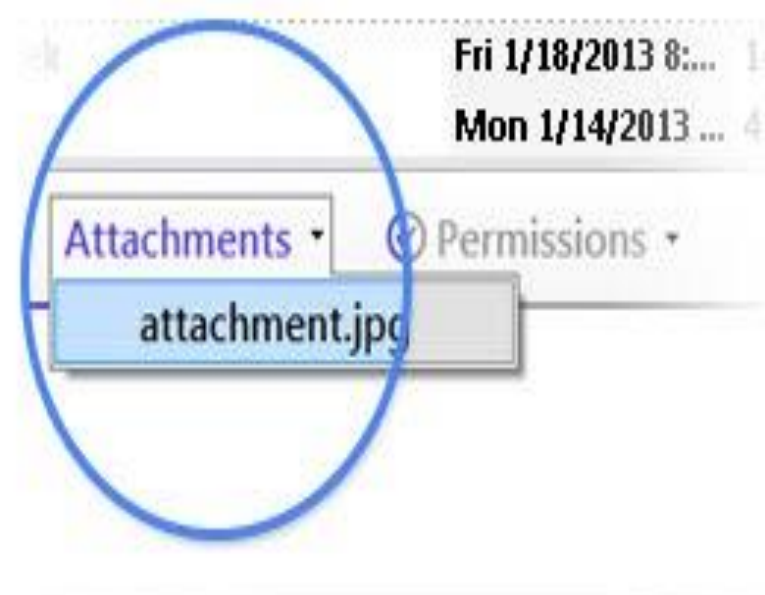
NEXT





# PRIVATE ATTACHMENTS

To view private attachments, look for the attachments dropdown, select the file to decrypt, then it will download to your computer.



**FINISH AND CLOSE WINDOW**

From: postmaster@virtru.com  
To: kenneth@raggiolaw.com  
Cc:  
Subject: Re: test virtru

Sent: Fri 11/28/2014 1:12 PM



Retezt

---

 The contents of this reply are not encrypted. Ask [kenraggio49@yahoo.com](mailto:kenraggio49@yahoo.com) to secure their emails with Virtru for free at [www.virtru.com](http://www.virtru.com).



# Receiving a Virtru Message

## Activate Virtru in Firefox for Windows

noreply-activation@virtru.com

Sent: Mon 11/3/2014 2:42 PM

To: kenneth@raggiolaw.com



PLEASE CONFIRM VIRTRU ACTIVATION

Hi [kenneth@raggiolaw.com](mailto:kenneth@raggiolaw.com),

You have received this email as part of Virtru's activation process. We want to make sure that you are you (and not someone pretending to be you)!

**ACTIVATE  
ME**

Click this button to complete your Virtru activation in  
**Firefox for Windows.**

If you did not request this activation, please do not click the button, and contact us at [support@virtru.com](mailto:support@virtru.com).

Thanks!  
The Virtru Team

You have received this message as part of Virtru's secure email service. For more information about Virtru, please

## Google Encryption

[gordon@gordoncruselaw.com](mailto:gordon@gordoncruselaw.com)

Sent: Mon 11/03/2014 2:40:13 PM

To: Ken Raggin

You are reading a secure message, protected by Virtru

Dear Ken,

Here's an encrypted email and an attachment.

Gordon D. Cruse, Esq.  
Gordon D. Cruse, **APLC**  
402 W. Broadway, Suite 1210  
San Diego, CA 92101-8508

Phone: 619-696-9922

Fax: 619-696-0586

[gordon@gordoncruselaw.com](mailto:gordon@gordoncruselaw.com)

[www.gordoncruse.com](http://www.gordoncruse.com)

Certified Family Law Specialist

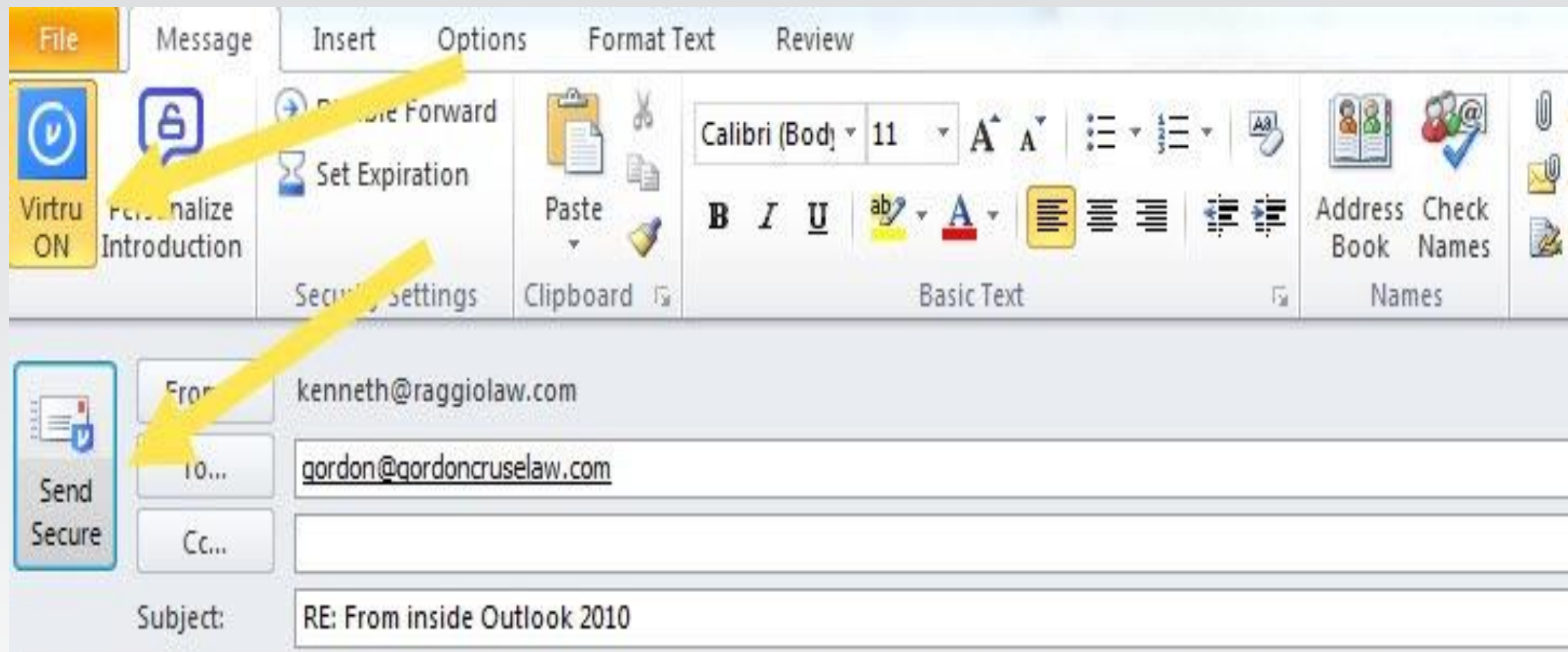
California State Bar Board of Legal Specialization

~ Fellow, American Academy of Matrimonial Lawyers

Gordon D. Cruse



# Virtru On



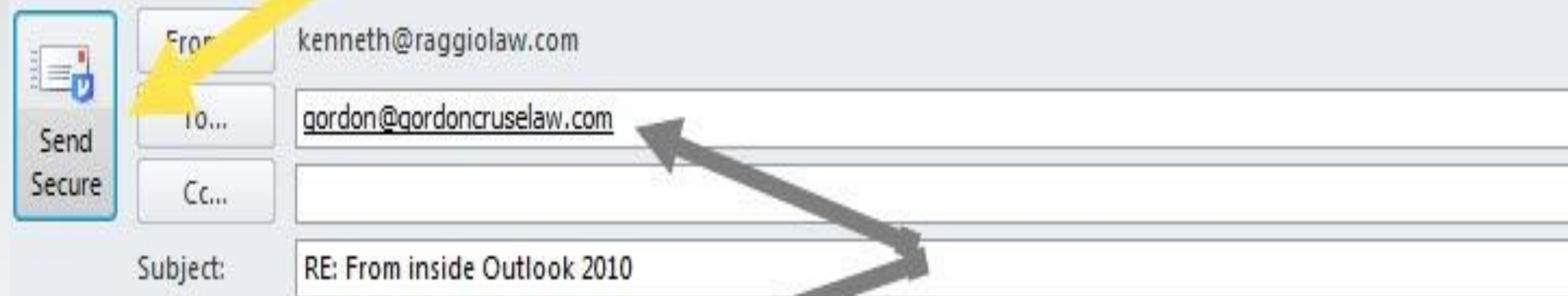
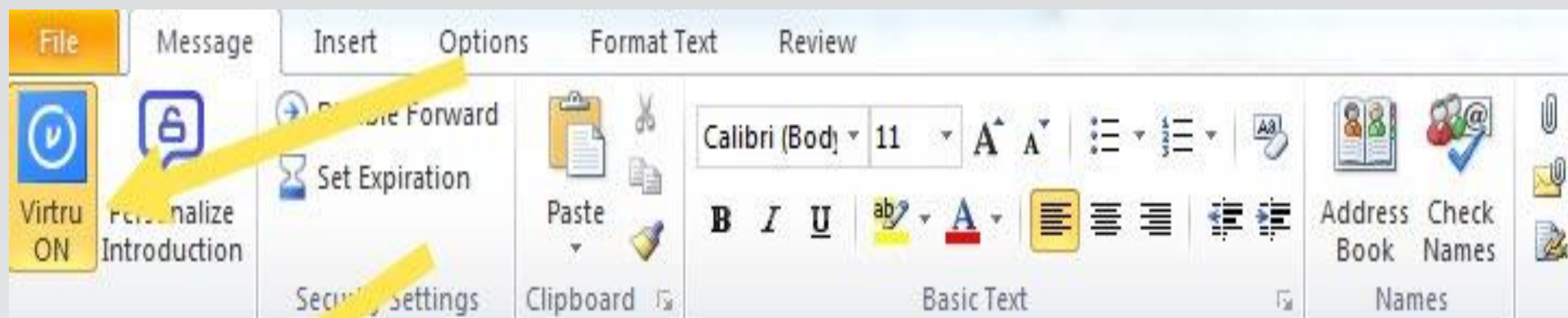
And I am replying directly from my email without any reference to the virtru postmaster like when I got your email

**From:** postmaster@virtru.com [mailto:postmaster@virtru.com]

**Sent:** Friday, November 28, 2014 1:29 PM

**To:** kenneth@raggiolaw.com

**Subject:** Re: From inside Outlook 2010

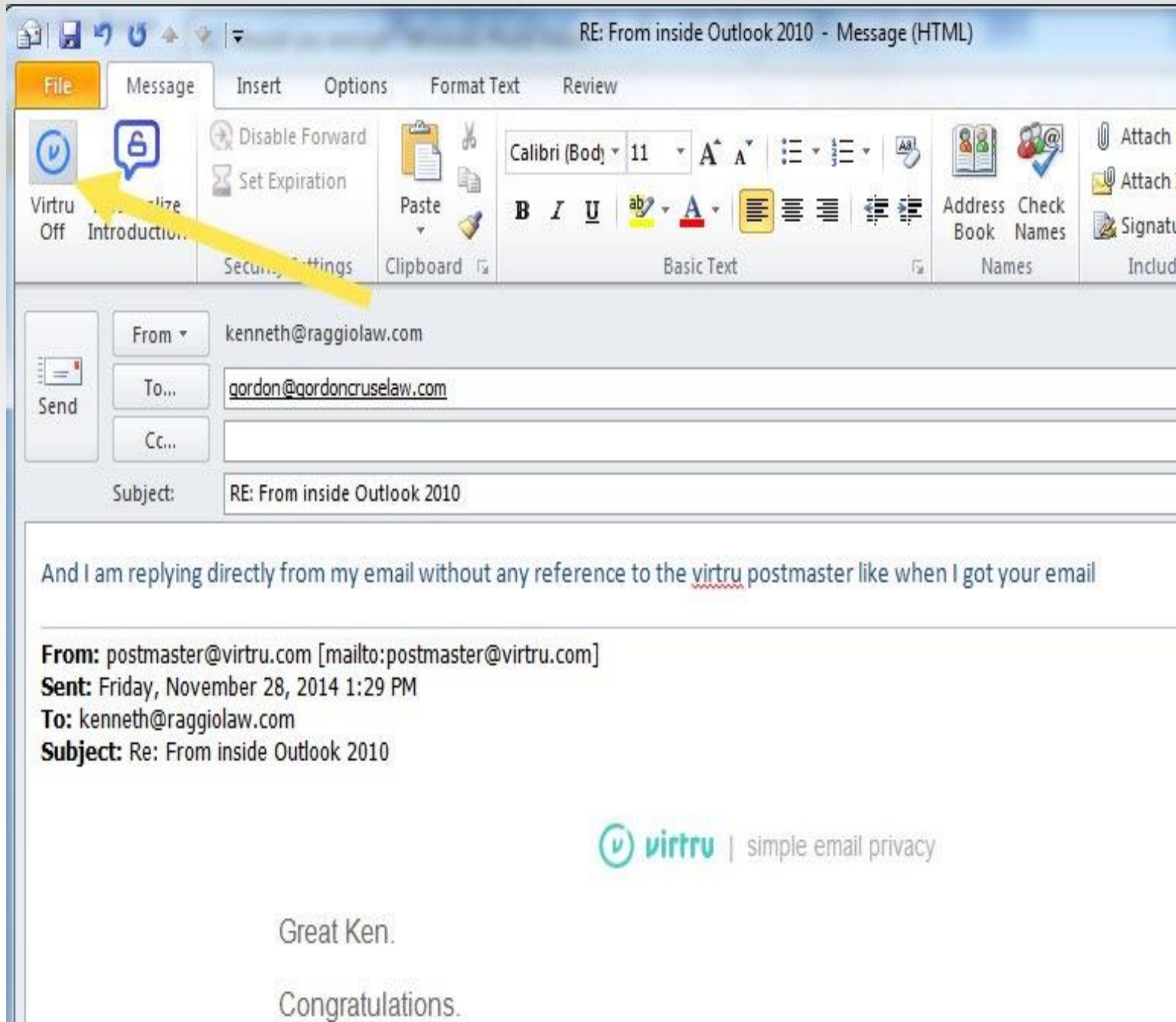


And I am replying directly from my email without any reference to the virtru postmaster like when I got your email

**From:** postmaster@virtru.com [mailto:postmaster@virtru.com]  
**Sent:** Friday, November 28, 2014 1:29 PM  
**To:** kenneth@raggiolaw.com  
**Subject:** Re: From inside Outlook 2010



# Sending Non-Encrypted Emails



# Social Media Worksheets

## INSTRUCTIONS FOR COMPLETION OF YOUR SOCIAL MEDIA WORKSHEET

As you are probably aware, social media has become tremendously popular in recent years, and most people these days have Facebook, Twitter, Pinterest, Tumblr, Instagram, etc. accounts. The impact of these types of accounts can certainly be seen in Family Court cases – sometimes for the better and sometimes for the worse.

In some cases, it can be helpful to run a background search on the opposing party's social media accounts, as doing so can help uncover evidence that can be used to help prove your allegations and/or disprove theirs. The more accurately you provide the requested information, the better chance we have of conducting a thorough search. Finding evidence like this can sometimes make a significant difference in the outcome of some cases.

We may also run a similar background search on your social media accounts as well in order to try to identify anything on your social media profiles that could be problematic for you. We understand that this type of information could potentially be embarrassing, but it is crucial that you be honest and disclose the requested information to us. Identifying and discussing problematic information now can provide an opportunity to minimize any possible damage to your case.

We believe that when you are facing or involved in a Family Court case, the best and most prudent course of action is to stop using social media accounts until your case is concluded. If you decide to ignore this advice and continue using them anyway, please immediately check to make sure that the privacy settings on all of your accounts are updated to provide the maximum protection. See [tiny.cc/FacebookPrivacy1](http://tiny.cc/FacebookPrivacy1) & [tiny.cc/FacebookPrivacy2](http://tiny.cc/FacebookPrivacy2) for more information and be mindful of the following:

- Anything that you place onto a social media account (or allow others to place onto your account) could be used against you in your case, sometimes with devastating results.
- Remember that it is very easy for postings to be taken out of context and/or interpreted differently than the way that you may have intended. Judges don't always have the same sense of humor that you do.
- Items posted to social media accounts can sometimes survive indefinitely, many times even after you believe that they have been removed.
- Anything posted to social media accounts is subject to the discovery process and could possibly be found if searched for in the right place by the right person with the right tools.
- Be very careful what you communicate to your online "friends" and the manner in which you do so, because often times these "friends" can end up providing information to the opposing party behind your back.

Please fully complete each item below as accurately and with as much detail as possible. Our ability to locate this type of information is extremely dependent upon our having the correct spelling for each type of account, and one letter can make all the difference in the world. If you don't know or don't have access to certain information, please put "unknown" or "???" to identify it as something we will need to try to locate and so that we will have the opportunity to discuss with you the best way to do so. When you have completed this worksheet, every question should be answered "yes", "no", "unknown", or "???". Please feel free to attach additional sheets and information as needed.

Again, we understand that the information requested in this worksheet is personal and can be potentially embarrassing to you. However, keep in mind that all information provided to our office is confidential, and we are asking these questions in order to obtain information necessary to assist us in providing the best possible representation in your case.

We have seen too many cases over the years be severely affected because someone never thought that “  x  ” would be discovered or used against them. We don’t want yours to become one of those, which is why we prepared this worksheet. If there is evidence out there on social media, we need to know about it and know about it now, not later. Information that leads to evidence we can use against the opposing party could help bolster your case. On the other hand, if there is information damaging to your case, we may be able to minimize its impact if we know about it now – before it’s too late.

Again, we strongly encourage you to refrain from participating in social media sites and apps during the course of our representation. Information found on social media sites and apps is not private, can be discoverable, and if used as evidence may be potentially damaging to your interests. It is important to understand that any information shared with others, whether verbally, in writing (via email, text message or letter), or posted online could result in a waiver of the attorney-client privilege. In addition, you should not delete or remove information from any social media sites, as doing so could be considered destruction of evidence, spoliation of evidence, or obstruction of justice.

We also advise you to refrain from communicating with us on any device provided by your employer or any computer, smartphone, or other device that is shared with someone else. In addition, when communicating with us, do not use your work email address or a shared email account. You should only use a private email account that is password protected and only accessible from your own personal smartphone or computer.

If you choose to ignore our advice, you are doing so at your own risk, with the full knowledge that doing so could negatively impact your case. If you have any questions or concerns about social media and how it may affect your case, please schedule a time to meet with one of our attorneys at your earliest convenience.

**I acknowledge that I have read and understand the above statements and that the information contained in this worksheet is true and accurate to the best of my knowledge.**

\_\_\_\_\_  
**Signature**

\_\_\_\_\_  
**Date**



THE  
**STEVENS FIRM, P.A.**  
FAMILY LAW CENTER



## INFORMATION ABOUT YOUR SOCIAL MEDIA USE

Do you use any type of social media account(s) now or have you ever used any such accounts in the past? **Yes or No.** If so, please provide the username, email address, or other identifying information for each such account that you have used or accessed:

Type of Social Media Account	Have / Had Account?		Your Account Information
Facebook	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Twitter	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Instagram	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
SnapChat	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Pinterest	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
LinkedIn	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Flickr	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
YouTube	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Google+	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
MySpace	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Other: _____	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Other: _____	<input type="checkbox"/> Yes	<input type="checkbox"/> No	

Please use the space below to provide any explanation(s) or additional information about the above accounts that we need to know about or discuss further with you:

---



---



---



---



---

## INFORMATION ABOUT YOUR USE OF DATING SITES/APPS

At any time during or since your relationship with the opposing party, do you use or have you used any type of "dating" website or app? **Yes or No.** If so, please provide the username, email address, or other identifying information for each such site or app and use the space below to describe the circumstances surrounding your use of same.

Type of Dating Site / App	Have / Had Account?		Your Account Information
Match.com	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
eHarmony.com	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
POF.com (PlentyofFish)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
OkCupid.com	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
AshleyMadison.com	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
JDate.com	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Tinder app	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Grindr app	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
How About We app	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Tingle app	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Other: _____	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Other: _____	<input type="checkbox"/> Yes	<input type="checkbox"/> No	

Please use the space below to provide the circumstances surrounding your usage of these and/or any additional information that we need to know about or discuss further with you:

---



---



---



---



---

Who  
Knew ?



# Dad uses Find My iPhone to hunt and kill thug who stole son's iPhone

Buster Hein (11:47 am PDT, Aug 5th)



1.7k



554



199



# Call Spoofing

Visited Getting Started iPad Apps for Trial Latest Headlines Texas House of Repres...

'Spoofing' likely cause of 911 calls from phone line belonging to Katie Couric's late husband

At least 10 bogus emergency calls have come from Couric's residence and are likely because a third party is hijacking the calls, tricking caller IDs into thinking a certain number is making the call.

BY [JOE KEMP](#) / NEW YORK DAILY NEWS

THURSDAY, FEBRUARY 14, 2013, 10:09 PM

9 7 1 +1



# How It Works





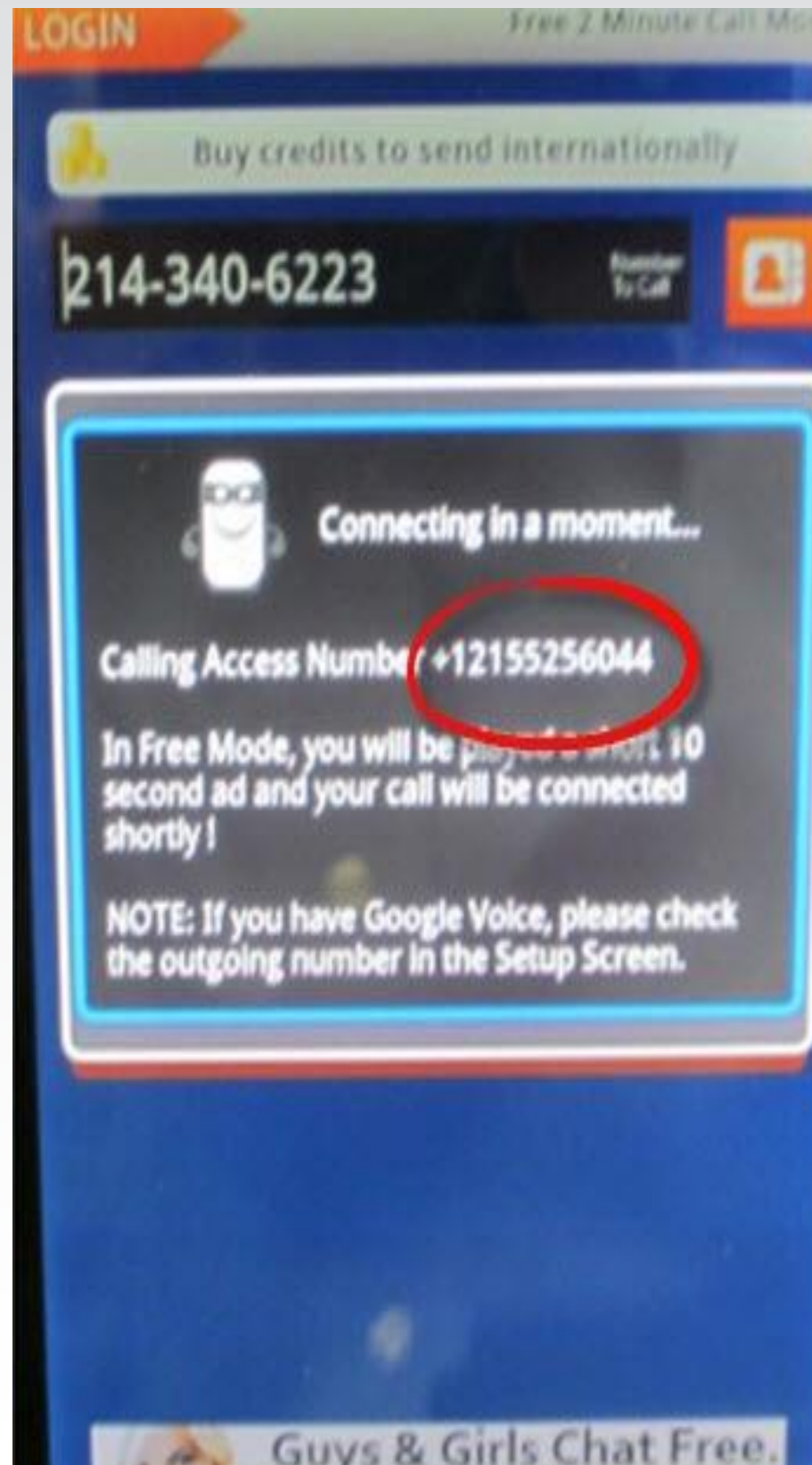
# App Opens



# Insert Desired Numbers



# Call Is Placed





# Authenticity = Admissibility?

## Lorraine v Markel Test

- Relevant
- Authentic
- Not hearsay
- Original or Duplicate
- Probative value v unfair prejudice

## Tienda v State Tests

- ESI (emails, chats, text messages admissible when sufficiently linked to purported author
- Distinctive Characteristics to admit over denial of authenticity
  - Nickname
  - Reference to RIP
  - Playing music from funeral

# Facebook Predicate

- Friends with / follow OP
- That's how you see their page
- Is [Exhibit] a screen shot of OP's Facebook page
- Fair and accurate
- Not changed in any way
- How do you know that OP, and not someone else posted the [Exhibit]
- Any reason to doubt posting was actually made by OP

OP = Opposing Party

# Tips & Takeaways

1. Educate your client from the beginning consultation about vigilance to protect their data and communications
2. Don't forget to mention their duty not to delete information or social media postings
3. Regularly remind clients of their continuing duty to preserve



# Tips & Takeaways

4. Make clients aware of how easy it is to “mine” data from their social media postings
5. Get client’s written consent to email communications
6. Suggest that a client do an “audit” or “sweep” of their electronic devices – phones, computers, and even vehicles

# Tips & Takeaways

7. Get a grip on passwords, password retention, and password changes
8. Turn it off when not using it. Or at least log off.
9. Have regular IT audits of your internal data security and backup systems
10. Encrypt

# Tips & Takeaways

11. Fill out the Audit letter

12. Follow the advice you give

13. Know when you need an ESI expert

14. Know what to do if you can't afford the expert



# practical (and understandable) ways to protect yourself and your clients from 21st century headaches

Kenneth G. Raggio  
Dallas, TX

J. Benjamin Stevens  
Spartanburg, SC

Susan Saper Galamba  
Overland Park, KS

Todd M. Frankfort  
Houston, TX

