

Welcome to the LSNC Webinar: “Technology and Client Confidentiality”

Legal Services of Northern California

April 15, 2011

- Robert Stalker, Managing Attorney
- Brian Lawlor, Regional Counsel
- Mark Sawyer, IT Manager

What “technology”?

Internet » Web » “The Cloud”

Pika CMS
Google Apps

Smartphones
Tablets
Other “mobile devices”

Laptops
Netbooks

USB flash drives
Portable hard drives

The Set-up

So you can get real work done from home, you've created duplicates of your client work files and stored them on the family computer...

“Hey, the easiest way for me to get work files from point A to point B is to use a portable USB drive.”

At the office you use Gmail to
answer a client's question...

Using Google Docs, you “share” a proposed settlement agreement with other counsel so they can review the document...

You love your laptop, but what you
you *really* love is how easy it is to
login automatically without having
to remember... *whatever!*

You're totally with the whole
"24/7 working in the Cloud" thing,
so while sipping a *latte* at Starbucks,
you flip open your laptop to check a
client's Pika case record...

You're at the airport, bored with playing "Angry Birds" on your iPhone, so you decide to use the free WiFi to check your Gmail...

You're *still* waiting at the airport
and you need to go to the
restroom, so you ask someone to
watch your laptop for a minute
while you're gone...

Finally, you get on the plane and pop open your laptop to get some work done during the flight...

The Issue

*"Does an attorney violate the duties of **confidentiality** and **competence** he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?"*

California State Bar, Formal Opinion No. 2010-179

Technology is ethically agnostic.

Technology is not the issue.

What matters is how **you** use it.

Client Confidentiality 101

An attorney has the duty ...

“to maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client”

Business & Professions Code, Section 6068(e)(1)

“The duty of confidentiality has very few exceptions.”

Rule 3-100, California Rules of Professional Conduct

Corollary duty of competence ...

“A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure....”

Rules 1.1, 5.1 and 5.3, Model Rules of Professional Conduct

“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.”

Comments to Rule 1.6, Model Rules of Professional Conduct

*“This duty, however, 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.”*

Comments to Rule 1.6, Model Rules of Professional Conduct

6

**factors to evaluate whether
there is an “undue risk of
unauthorized disclosure”**

1.

The level of security and whether reasonable precautions may be taken to increase the level of security.

Formal Opinion 2010-179, Section 3(a)

2.

The legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information.

Formal Opinion 2010-179, Section 3(b)

3.
**The degree of sensitivity of the
information.**

Formal Opinion 2010-179, Section 3(c)

4.

The possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product.

Formal Opinion 2010-179, Section 3(d)

5.
The urgency of the situation.

Formal Opinion 2010-179, Section 3(e)

6.

The client's instructions and circumstances, such as access by others to the client's devices and communications

Formal Opinion 2010-179, Section 3(f)

**Reconciling these duties with
current technologies**

Using PUBLIC wireless connections

Due to the lack of security features provided in most public wireless access locations, an attorney risks violating his duties of confidentiality and competence in using public wireless connections **unless he takes appropriate security precautions.**

Using PUBLIC wireless connections

Depending on the sensitivity of the matter, an attorney **may need to avoid using the public wireless connection entirely**, or notify the client of possible risks attendant to his use of the public wireless connection, and seek her **informed consent** to do so.

Using PRIVATE wireless connections

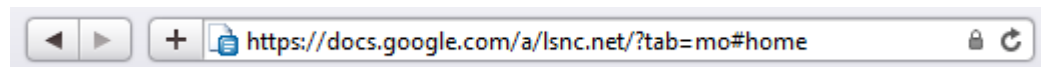
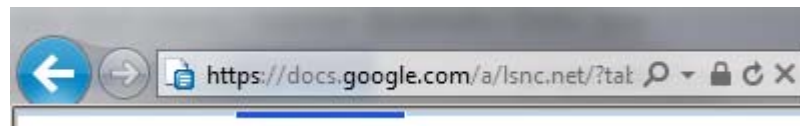
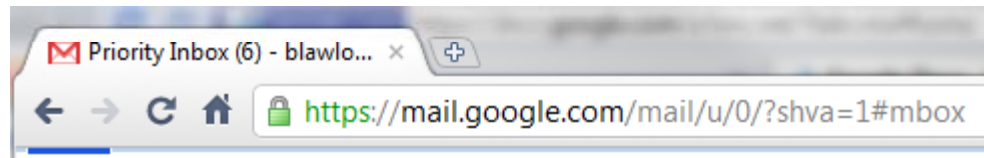
Assuming an attorney's personal wireless system has been configured with appropriate security features, the attorney would not violate his duties of confidentiality and competence by working on a client's matter at home.

Making your devices secure

(the following assume you are using the device for client-related work)

1. “Lock” icon = encrypted connection

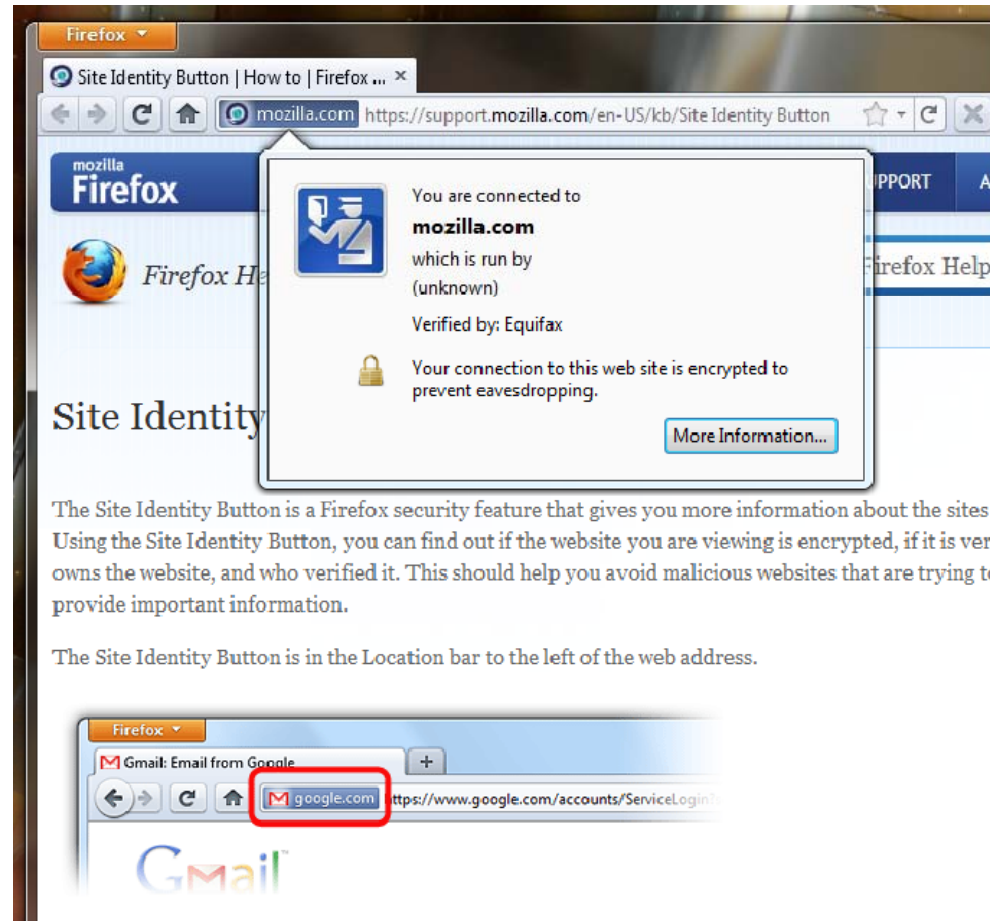
1. Firefox 3.x
2. Google Chrome
3. Internet Explorer
4. Safari



1. “Lock” icon = encrypted connection

Firefox 4.x is different

Click on the **Site Identity** button to the left of the web address to see the level of security and whether the site is encrypted.



2. LSNC desktops behind the firewall

You're good... because LSNC network protocols require a secured login.

You do not have to take any extra security precautions if you are accessing Pika, Gmail or other Google Apps or the local F: drive from your office desktop.

3. Laptops



<http://www.truecrypt.org/>

- ✓ Regardless of location, the laptop must be encrypted with **TrueCrypt** software.
- ✓ All LSNC laptops will always be encrypted using TrueCrypt.

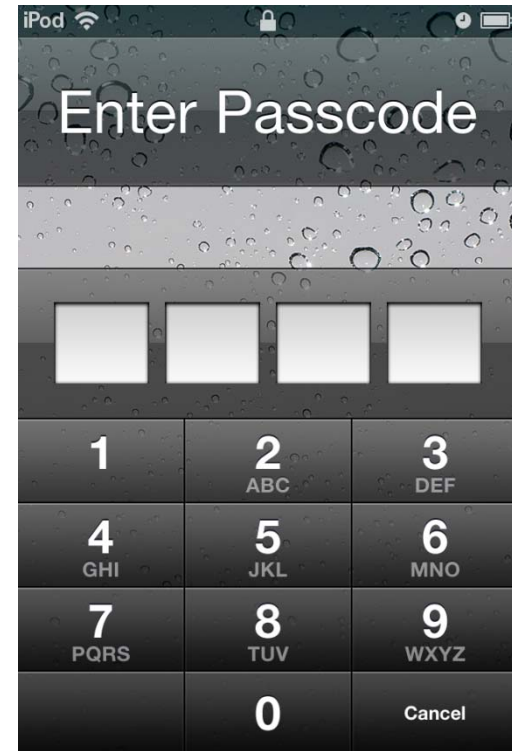
3. Laptops

If you use a personal laptop, you **must use TrueCrypt** to encrypt the entire laptop.

For instructions on how to encrypt your laptop, see the “How to encrypt your laptop” tutorial online at the SPN.

4. Smartphones + Mobile Devices

If you use a web-enabled smartphone or other mobile device, you must activate the device's “passcode lock” feature... whatever.



5. Your home desktop

If your home computer is web-connected, you must use a **firewall**.

If your Internet connection at home is wireless-enabled, the **wireless connection** cannot be open. It **must be secure and password protected**.

*Consider using **TrueCrypt** for your home computer. You can download TrueCrypt via the SPN.*

5. Your home desktop

If others have physical access to your desktop...

- ✓ All client folders and files must be encrypted; **and**
- ✓ You must manually login to Pika and Google Apps each time you use them; **and**
- ✓ You may not allow your browser to “remember” or “save” your Pika or Google Apps login information; **and**
- ✓ You cannot leave your browser session open after you are finished using Pika or Google Apps – you must close your browser each time you use it.

6. USB or other portable drives

If you use a portable drive to transport client-related files from the office to an outside location (including your home), you must use an encrypted USB or other portable drive.

LSNC will provide all offices with one or more 2G “Blackbox” USB flash drives that are natively encrypted.

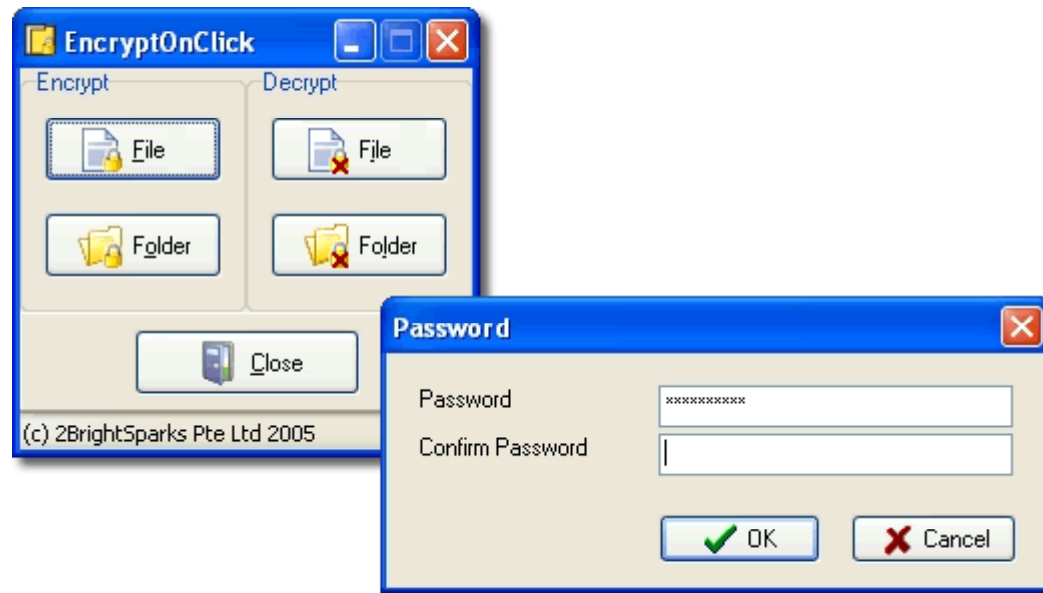


6. USB or other portable drives

If you need a larger encrypted portable hard drive, contact Mark or Ed.

If an LSNC-encrypted portable device is not available, you can use **EncryptOnClick** to secure the files or folders and then transport them on a USB flash or other portable drive.

6. USB or other portable drives



<http://www.2brightsparks.com/onclick/eoc.html>

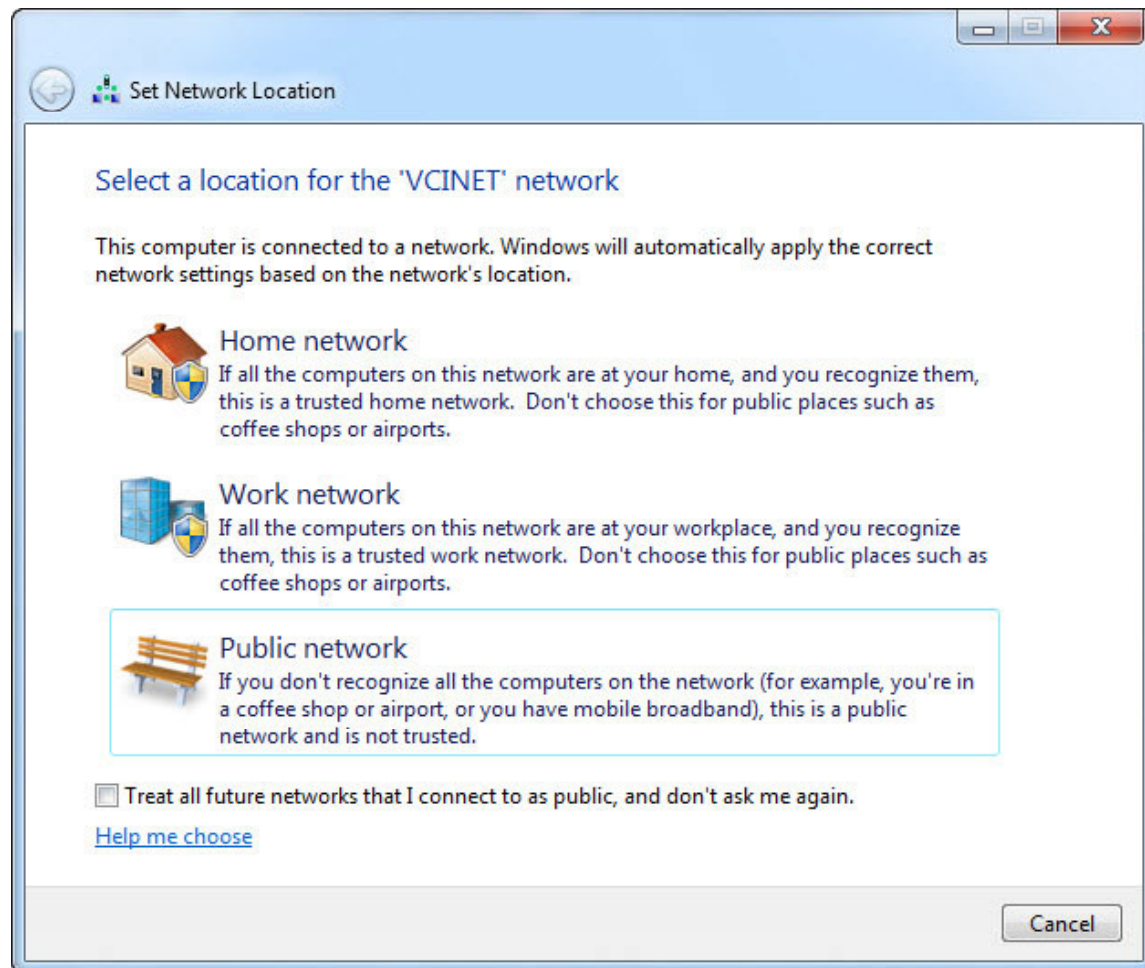
*You can download **EncryptOnClick** via the SPN.*

7. The “Starbucks” Scenario

- ✓ When relying on a **public wireless access point** – e.g., at Starbucks or an airport or a hotel – the presumption is that the web connection **may not be sufficiently secure** to perform client-related work or communications.
- ✓ To proceed, you must know more to assure you have a **reasonable expectation of privacy**.
- ✓ Do ***not*** configure your smartphone or mobile device to automatically connect to WiFi hotspots.

7. The “Starbucks” Scenario

Select:
“Public Network”



Behavioral Issues...

**“Pay attention to
what you’re doing”**

Technology and Client Confidentiality

Legal Services of Northern California

April 15, 2011

- Robert Stalker, Managing Attorney
- Brian Lawlor, Regional Counsel
- Mark Sawyer, IT Manager