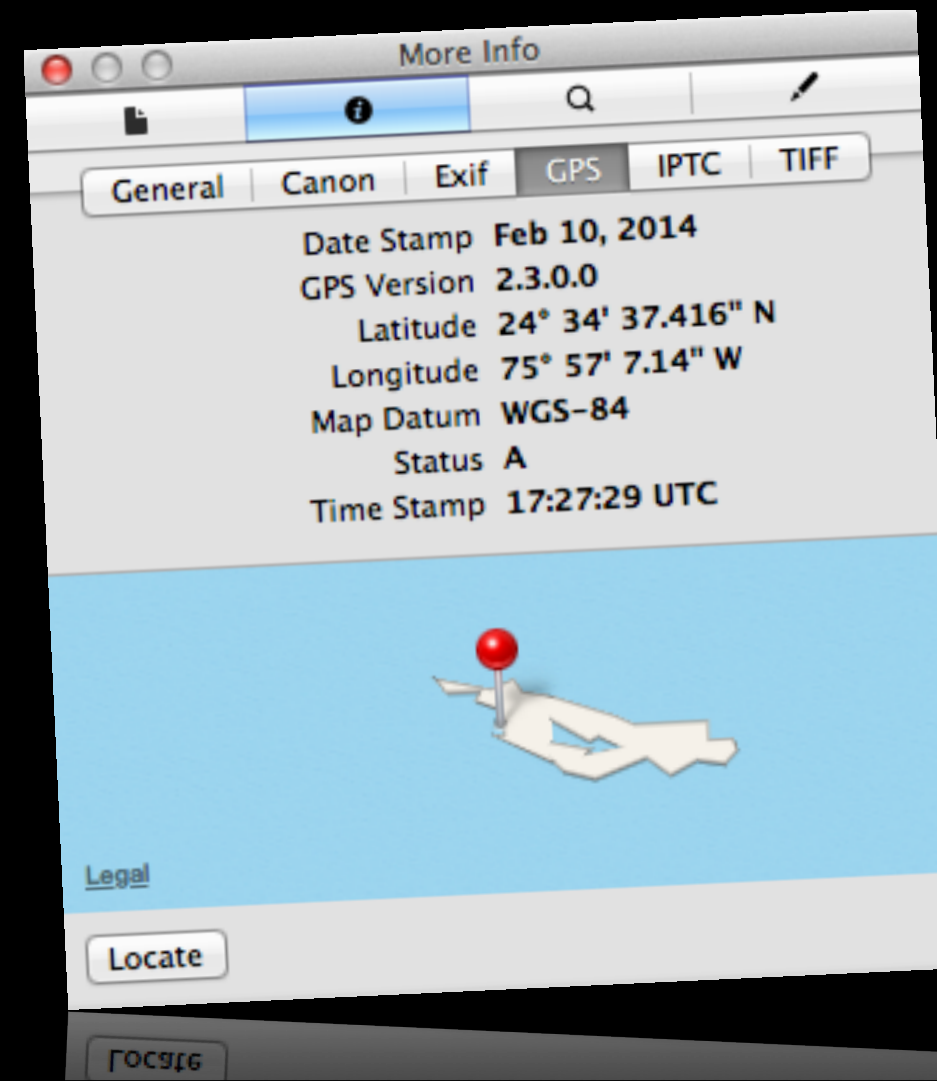




Cove Apple Club

February 26, 2014



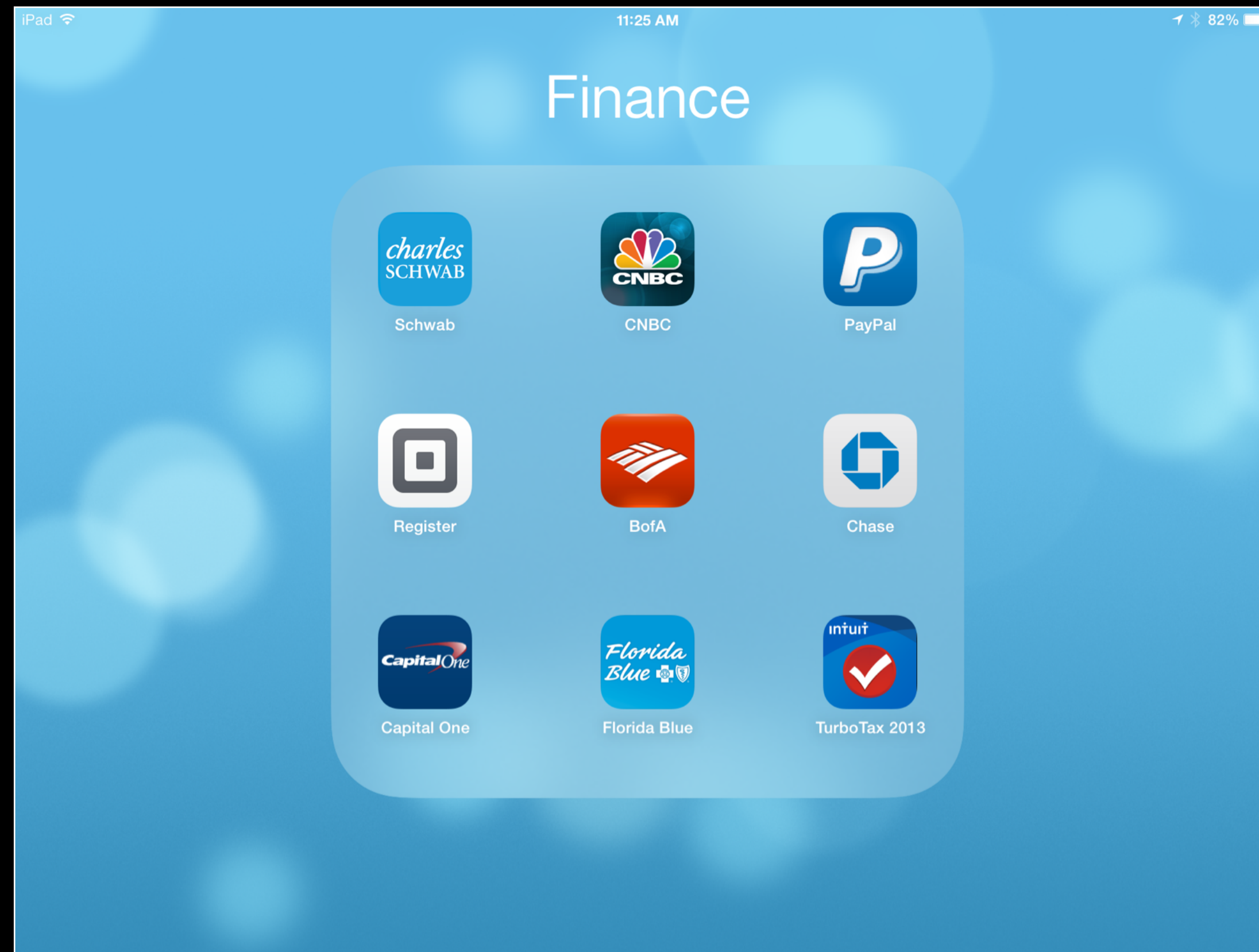
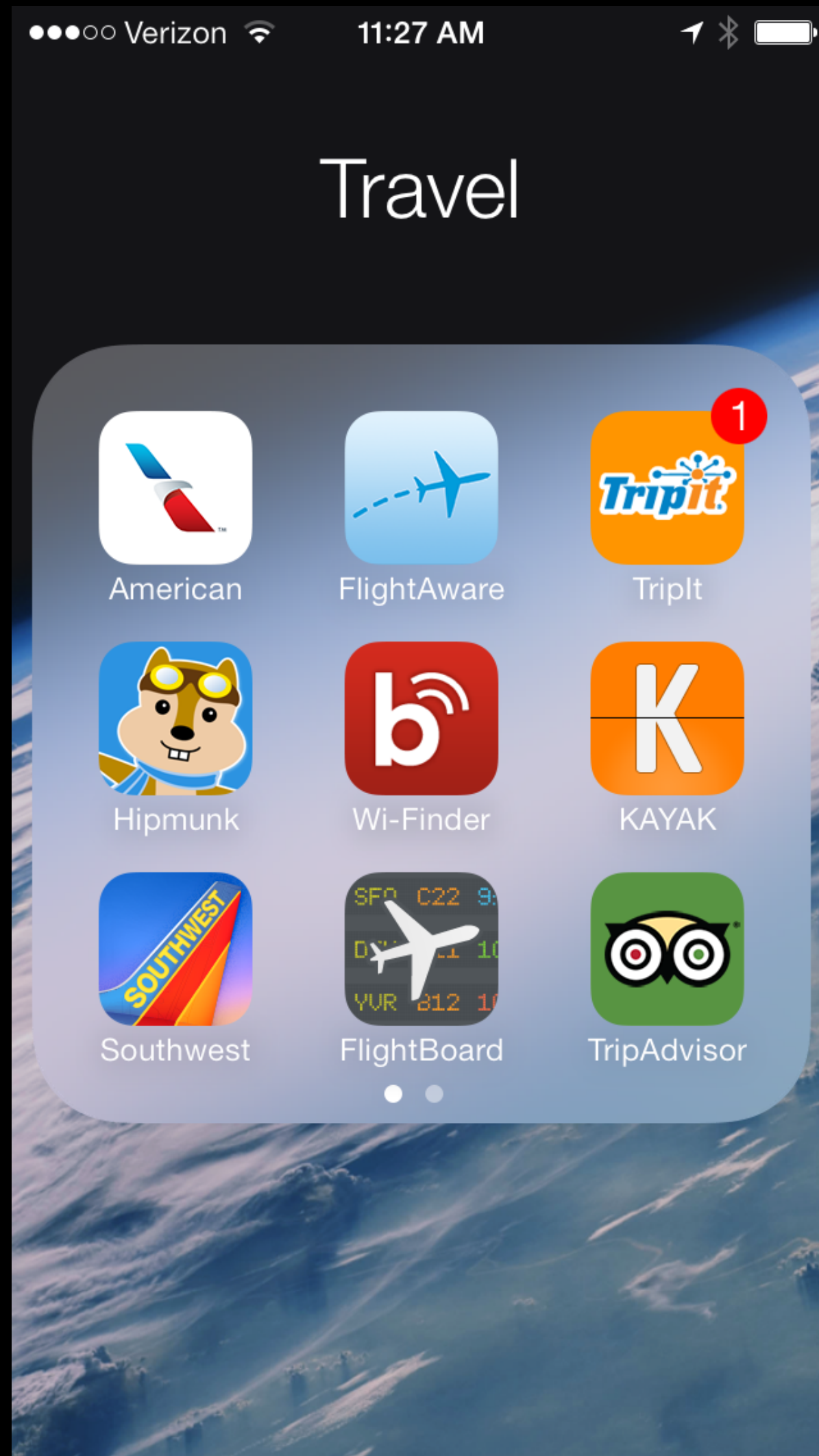
Tonight's Topics

- Managing app-sprawl on iOS with App Folders
- Apple's recent iOS & OS X Updates
- iCloud & Dropbox: Why you probably want both
- "It's Only Metadata!"

We Are Now Taking Requests!

- Do you have an idea for a Cove Apple Club topic you'd like to see presented?
- Shoot us an email at **info@coveappleclub.com** and we'll do our best to add it to the agenda for our next meeting!

Managing App Sprawl



This Week's OS Updates

- Apple pushed out iOS 7.0.6 on Friday, and OS X 10.9.2 last night
- Both contained numerous bug fixes, some new features (in OS X), and a major bug fix to how secure connections were handled in Safari
- This has become known in the past week as the “gotofail” vulnerability

gotofail code snippet

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer
signedParams,
                                uint8_t *signature, UInt16 signatureLen)
{
    OSStatus      err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```



```
OSStatus          err;
...

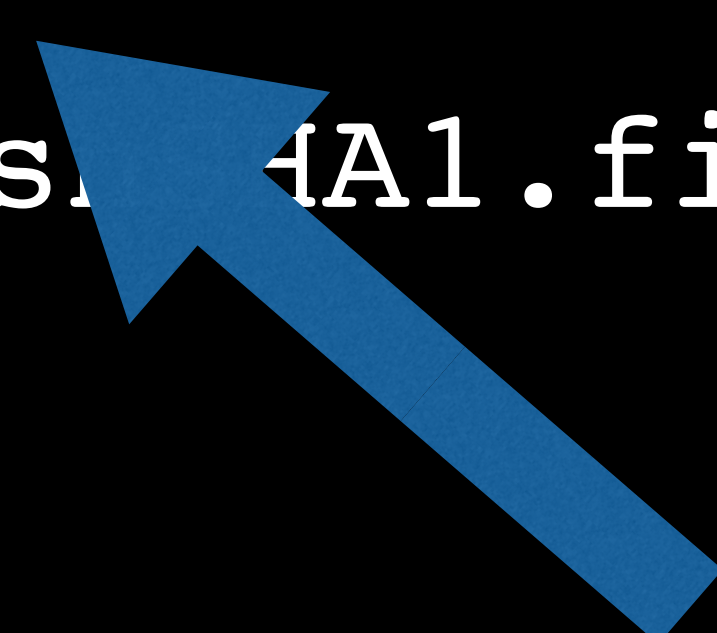
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom))
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams))
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

```
OSStatus          err;
...

if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom))
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams))
    goto fail;
goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

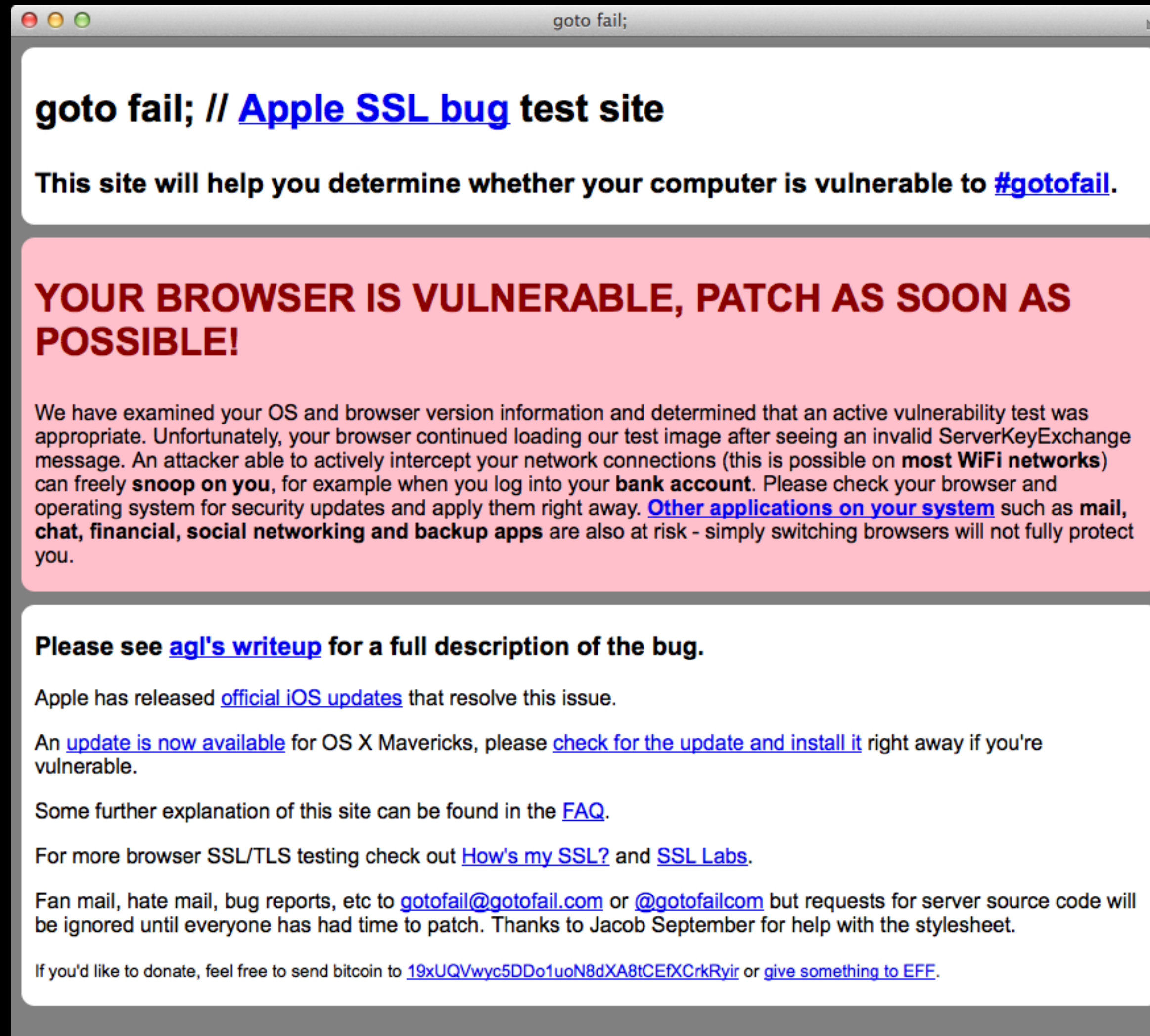


Error!
This line of code will always execute
SSL verification will always succeed

Net Result

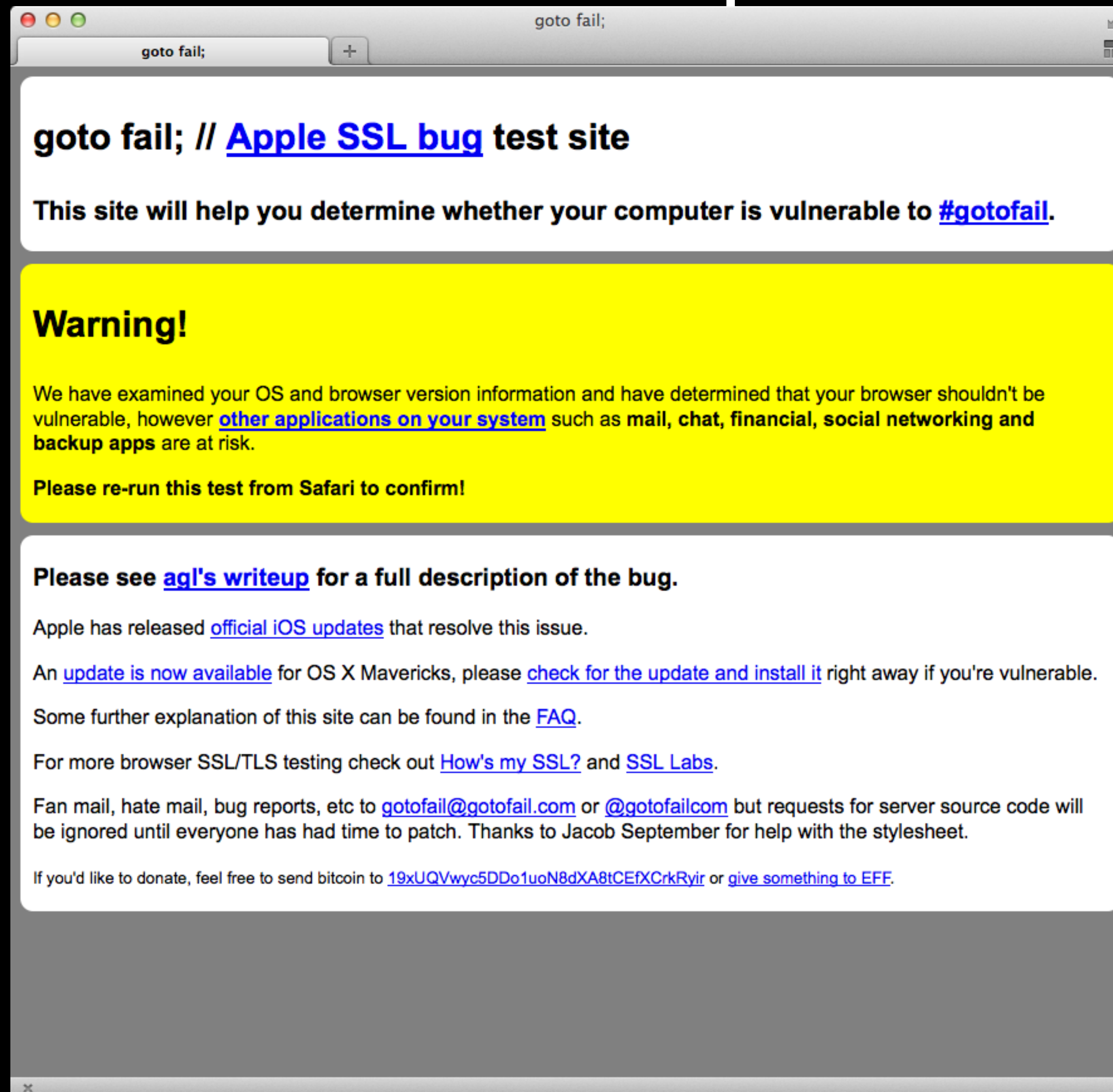
- An attacker with *specialized tools and knowledge*, in a *privileged network position*, could intercept network connections that passed TLS/SSL authentication when connecting to a secure site
- This vulnerability is theoretical only; no known attacks in the wild have been reported that exploit this vulnerability
- With the recent iOS and OS X updates, the vulnerability is fixed

Proof of concept: unpatched Safari



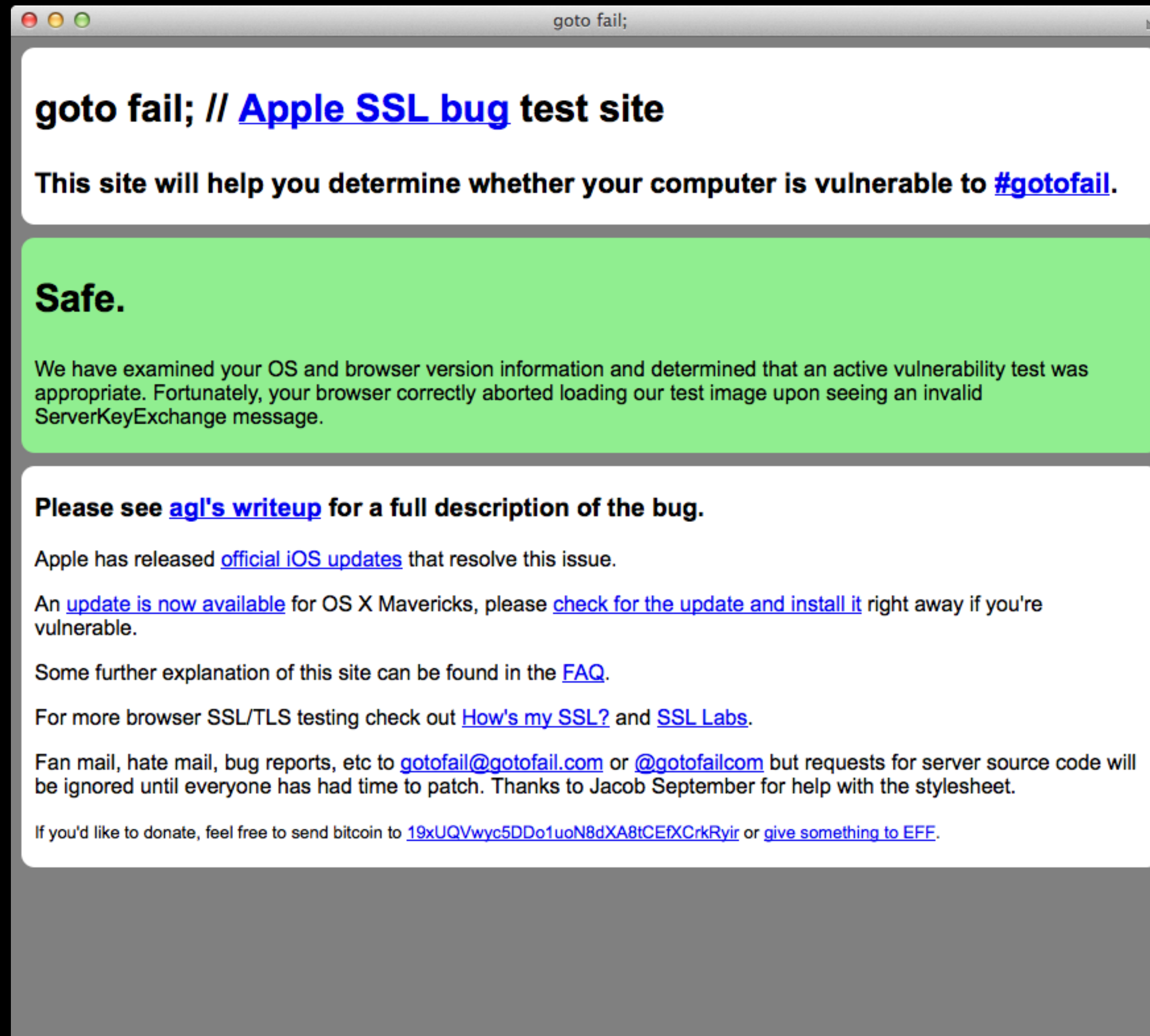
source: gotofail.com,
Safari in OS X 10.9.1,
2/24/14

Proof of concept: Firefox



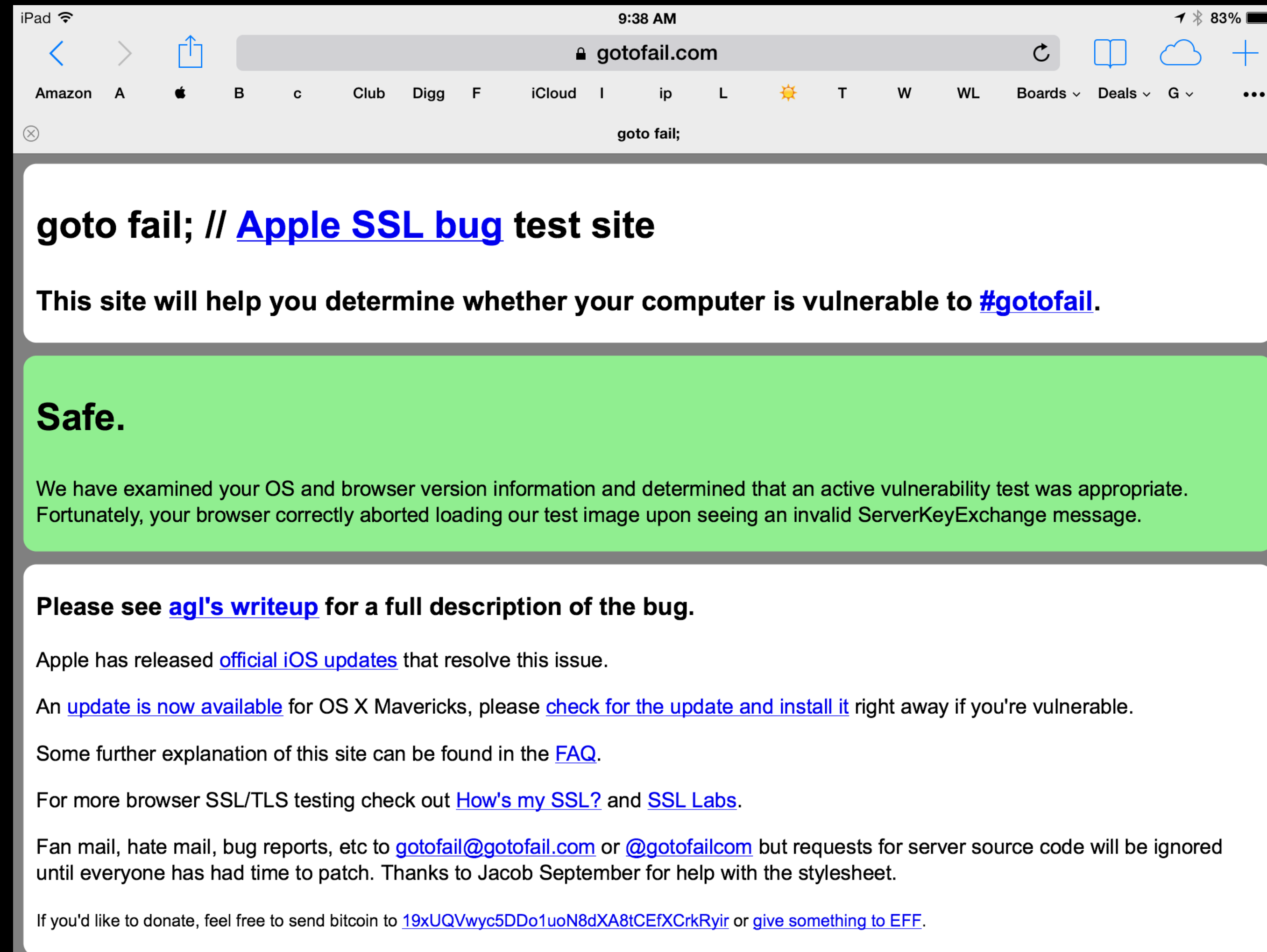
source: gotofail.com,
Firefox 28.0 in OS X
10.9.1, 2/24/14

Proof of concept: patched Safari



source: gotofail.com,
Safari in OS X 10.9.2,
2/25/14

Proof of concept: patched iOS



source: gotofail.com,
Safari in iOS 7.0.6,
2/25/14

gotofail Fix Timeline

- Apple has been testing 10.9.2 for at least six weeks; probably testing iOS 7.0.6 about as long or longer
- gotofail bug had not been disclosed anywhere until early last week
- By that time, Apple had pushed out two release candidate versions of 10.9.2, for which I am an AppleSeed Beta Tester
- Pushing out an update for a running OS to hundreds of millions of devices in dozens of languages is not a trivial matter

gotofail Fix Theories

- This bug did not exist in 10.9.0, or in iOS 6.0-7.0
- Experts seem to agree that this was an honest mistake (fixed by adding ***a single curly brace “{”*** in a codebase exceeding ***100,000,000*** lines of code)
- Apple does not credit an outside researcher for surfacing this bug, as they routinely do for other security fixes
- Some believe the bug was surfaced when Apple engineers reviewed their code after looking at the slides about NSA surveillance leaked by Edward Snowden

Meanwhile, on the Dark Side:

- Hundreds of millions of Windows users running Internet Explorer 9 or 10 are subject to a real-world attack propagating in the wild
- "If the attack is successful, the exploit drops a banking Trojan that steals login details from certain banks," the Symantec researchers said.
- Unpatched since 2/13/14

source: itworld.com
2/26/14

IE zero-day exploit being used in widespread attacks

February 26, 2014, 6:14 AM — The number of attacks exploiting a yet to-be-patched vulnerability in Internet Explorer has increased dramatically over the past few days, indicating the exploit is no longer used just in targeted attacks against particular groups of people.

The vulnerability affects Internet Explorer 9 and 10 and was publicly revealed on Feb. 13 by researchers from security firm FireEye who [found an exploit for the flaw](#) being served from the Veterans of Foreign Wars (VFW) website. Security researchers from security firm Websense [later reported](#) that the same vulnerability was being exploited from the compromised website of French aerospace association GIFAS (Groupement des Industries Francaises Aeronautiques et Spatiales).

Microsoft published [a security advisory](#) about the vulnerability, which is tracked as CVE-2014-0322, and released a "Fix It" tool [as a temporary workaround](#). However, the company has not yet released a regular patch through the regular Windows update channel.

The attacks reported by FireEye and Websense are known as "watering hole attacks" because they involve compromising websites visited by particular groups of people that attackers wish to target -- in these particular cases U.S. military personnel and French defense contractors.

particular cases U.S. military personnel and French defense contractors.
particular groups of people that attackers wish to target -- in these

iCloud & Dropbox

Life among the clouds

What is a “cloud”?

- A “Cloud” is a server sitting in a datacenter...
- ...that sends, receives, stores, computes or monitors data
- More typically, a cloud is a cluster of replicated servers sitting in separate, redundant, geographically distant data centers
- Many of our iOS and Mac OS services are cloud-based, cloud-enabled, or augmented by cloud computing & storage

Leading Cloud Providers

- Apple: proprietary cloud to support Apple customers only
- Amazon Web Services: provides the infrastructure that powers much of the Internet, including all of Dropbox, Netflix, Zynga, Evernote, Reddit, SmugMug, FourSquare, PhotoBucket, thousands more
- Microsoft Azure: public, private and government cloud services
- Google: public, private and government cloud services
- IBM, Oracle, Box.net, CA, Unisys, 1&1, GoDaddy, dozens more

Benefits of Cloud Computing

- No single point of failure
- Your data, in sync, on any device, anywhere, anytime
- Leverage the immense computing power of a cloud from your mobile device, desktop or laptop
- Send/receive, process, monitor, manage your data & services even when your device is off or offline



Benefits of iCloud

- 5Gb of free cloud storage for all Apple device owners
- No sign-up needed; uses same login credentials as iTunes or App Store
- Tightly integrated into the OS and all built-in apps on iOS and Mac
- Nothing to install/update/manage/fiddle with; “it just works”
- Simple, automatic storage and sync of nearly all data from all Apple apps & services

Some of Apple's Cloud Services



- Mail
- Contacts
- Calendar
- Reminders
- Notes
- Find My Friends
- Find My Mac
- iCloud Tabs
- iCloud Bookmarks
- iTunes Radio
- Siri
- iCloud Backup
- iCloud Keychain
- iWork for iCloud
- iTunes Match
- Back to My Mac
- ...and more



- Free, public cloud storage; 2Gb free, up to 100Gb paid
- Free apps for Mac, iOS, Windows, Android
- Works like a “regular” folder on your hard disk, but with one magical property
- Dropbox support is integrated into dozens of popular apps, using Dropbox as the storage-and-sync utility for the app’s data

Benefits of **Dropbox**

- 2Gb of free cloud storage
- Earn up to 14Gb of additional free space by referring friends
- Works on non-Apple ecosystem devices, if you have any
- Connects to dozens of third-party apps for data storage & sync (1Password, Scanner Pro, etc.)
- Behaves like a regular folder on your Mac
- Access your Dropbox via Dropbox apps or at dropbox.com



Demo



It's Only Metadata!



- Roger Clemens, entertainer
- Testified to Congress about whether he voluntarily squirted a legal, non-toxic substance into his butt
- Indicted on federal perjury charges related to his testimony
- Seven-year investigation, five-year prosecution, 10-week trial
- Acquitted on all felony charges



Let's Recap

- Roger Clemens is an entertainer who throws baseballs while people watch
- Has no criminal record, but is subpoenaed by Congress on suspicion of fibbing about his use of a legal substance
- Is questioned under oath about whether he did or didn't use this legal substance
- Criminally prosecuted on federal charges for what he said



- James Clapper, Director of National Intelligence
- Reports directly to the President
- He's the boss of the CIA *and* the NSA
- Top intelligence official in the US
- Takes an oath to “protect and defend the **Constitution of the United States**” against all enemies, foreign and domestic



Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, ***shall not be violated***, and no Warrants shall issue, but upon ***probable cause***, supported by Oath or affirmation, and ***particularly describing the place to be searched***, and the persons or things to be seized.

Clapper Before Snowden Leaks

- Clapper testifies under oath at the Senate Intelligence Committee on March 12, 2013
- Question by Senator Wyden (D-Ore): “Does the NSA collect ***any type of data at all*** on millions or hundreds of millions of Americans?”
- Clapper’s answer under oath: “No, sir.”
- We now know that was a lie, and Clapper had to know it was a lie.

source: *Congressional Record*,
NY Times

Let's Recap

- Clapper is a cabinet-level official of the US government, sworn to protect and defend the Constitution
- He testified under oath before a US Senate committee in his official capacity as Director of National Intelligence
- He lied under oath when asked a direct question by a US Senator, and we now know it is a lie
- DNI Clapper has not be indicted, prosecuted or tried for his perjury before Congress, as was show business personality Roger Clemens

source: *Congressional Record*,
NY Times

Thanks to Snowden, We Now Know:

- NSA has been hoovering up “metatdata” on ***trillions*** of phone calls, Internet connections, Web browsing sessions, *the entire address books*, text messages and emails ***of US citizens***, for years, without individualized suspicion and without a court-ordered warrant
- Clapper defends this unauthorized, unconstitutional, secret and unprecedented domestic surveillance program targeting US citizens with the claim that “it’s only metadata!”

How Bad Is It?

- The government's ***own privacy watchdog***, "The Privacy and Civil Liberties Oversight Board," calls the NSA's "215" program ***illegal***, says it has "has gone beyond its statutory authority and needs to be modified."
- PCLOB says, "For now, it should be discontinued until a legal alternative is approved by Congress."



How Bad Is It, Part II:



Note: This is not a joke

source: <http://www.nsa.gov>

It's Only Metadata!

- What ***is*** metadata?

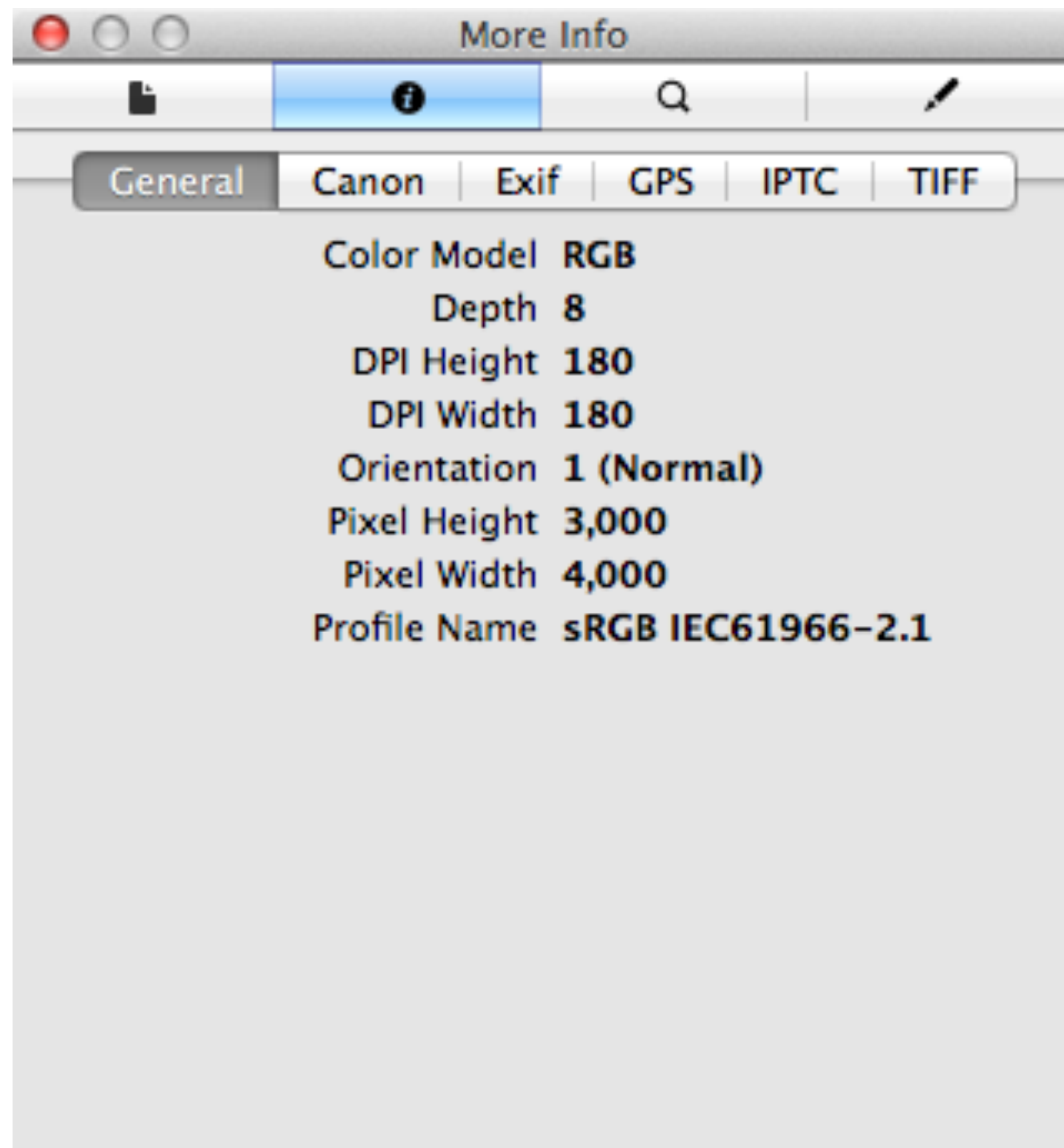


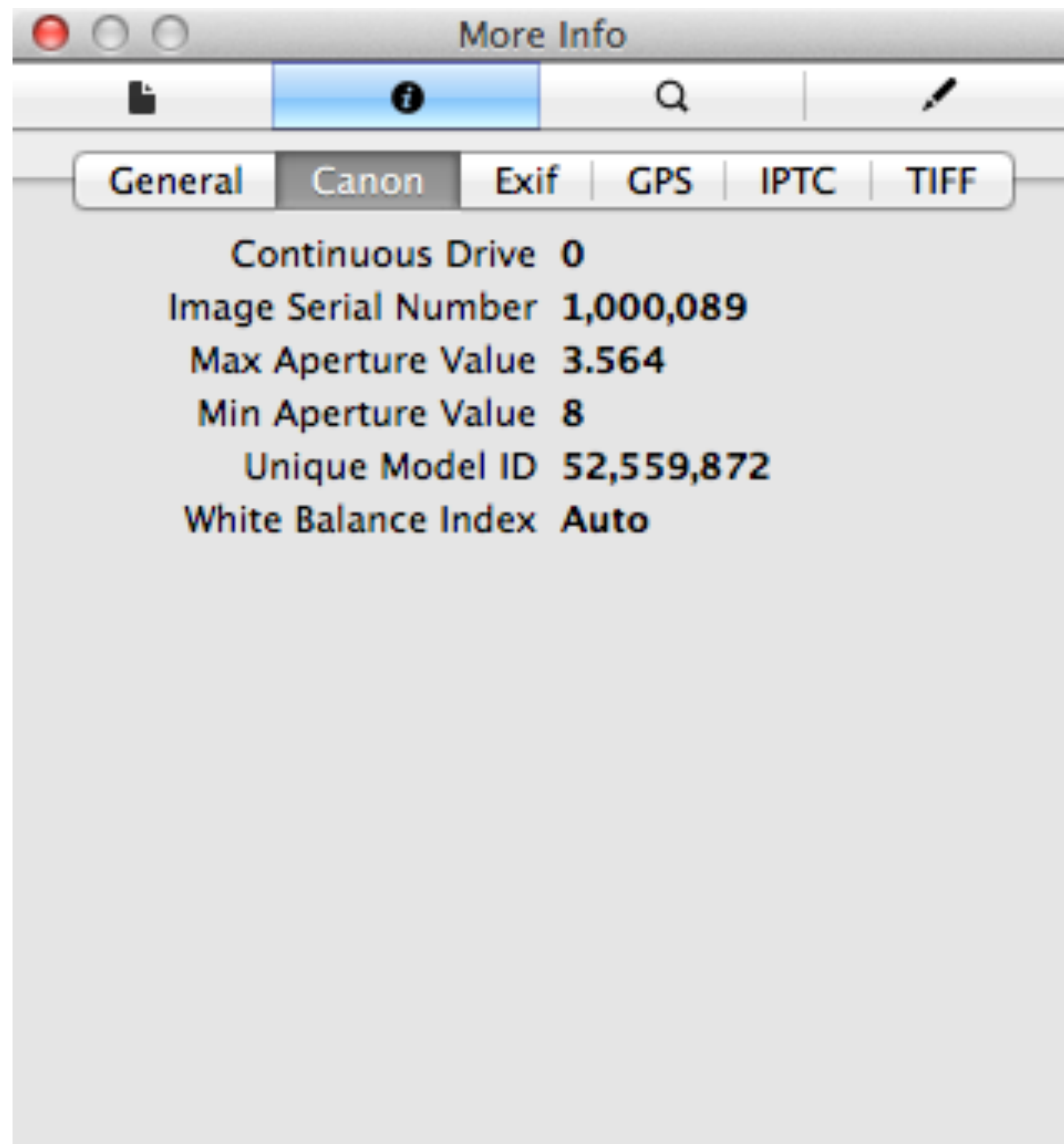
A photo is *data*

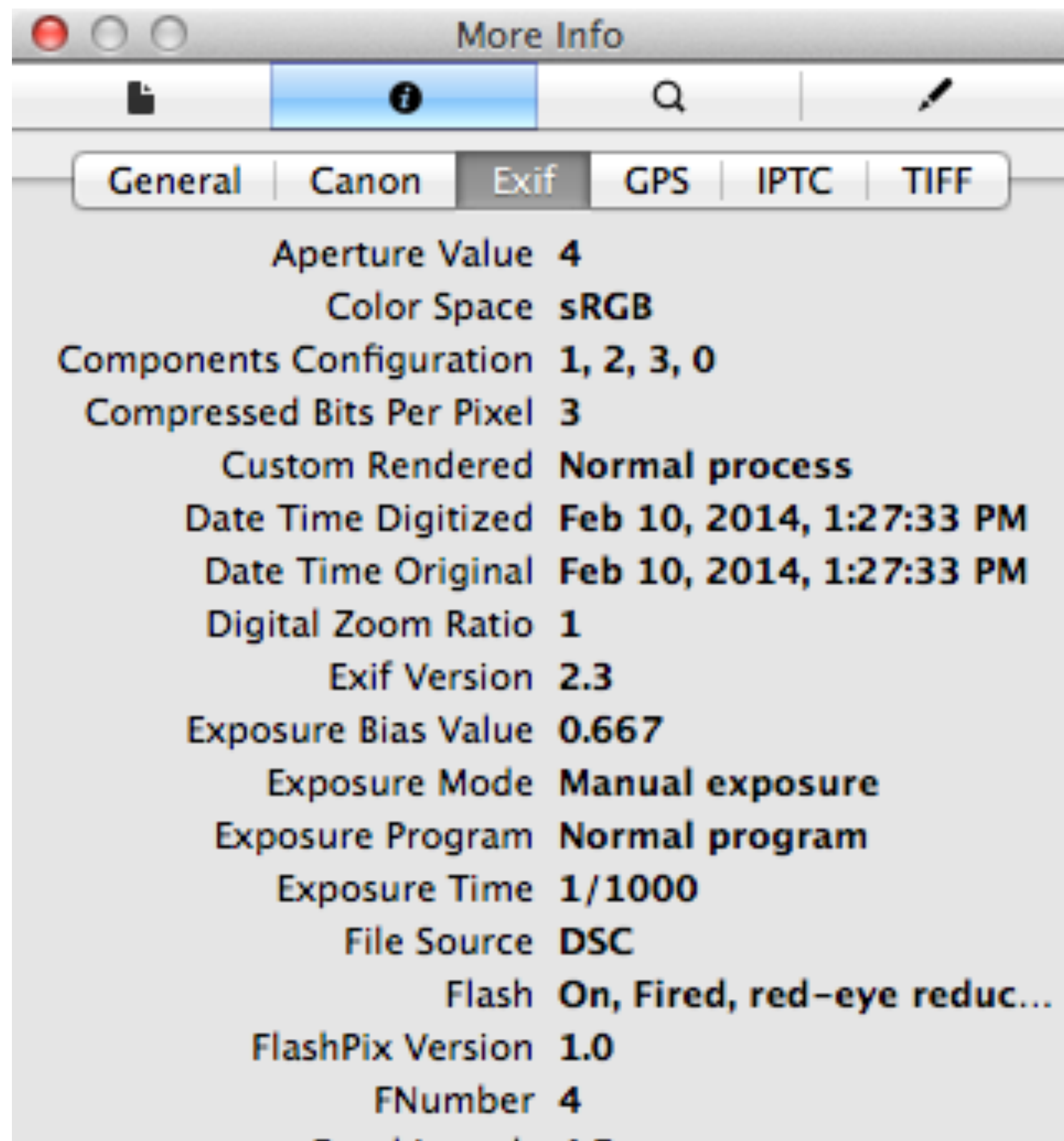


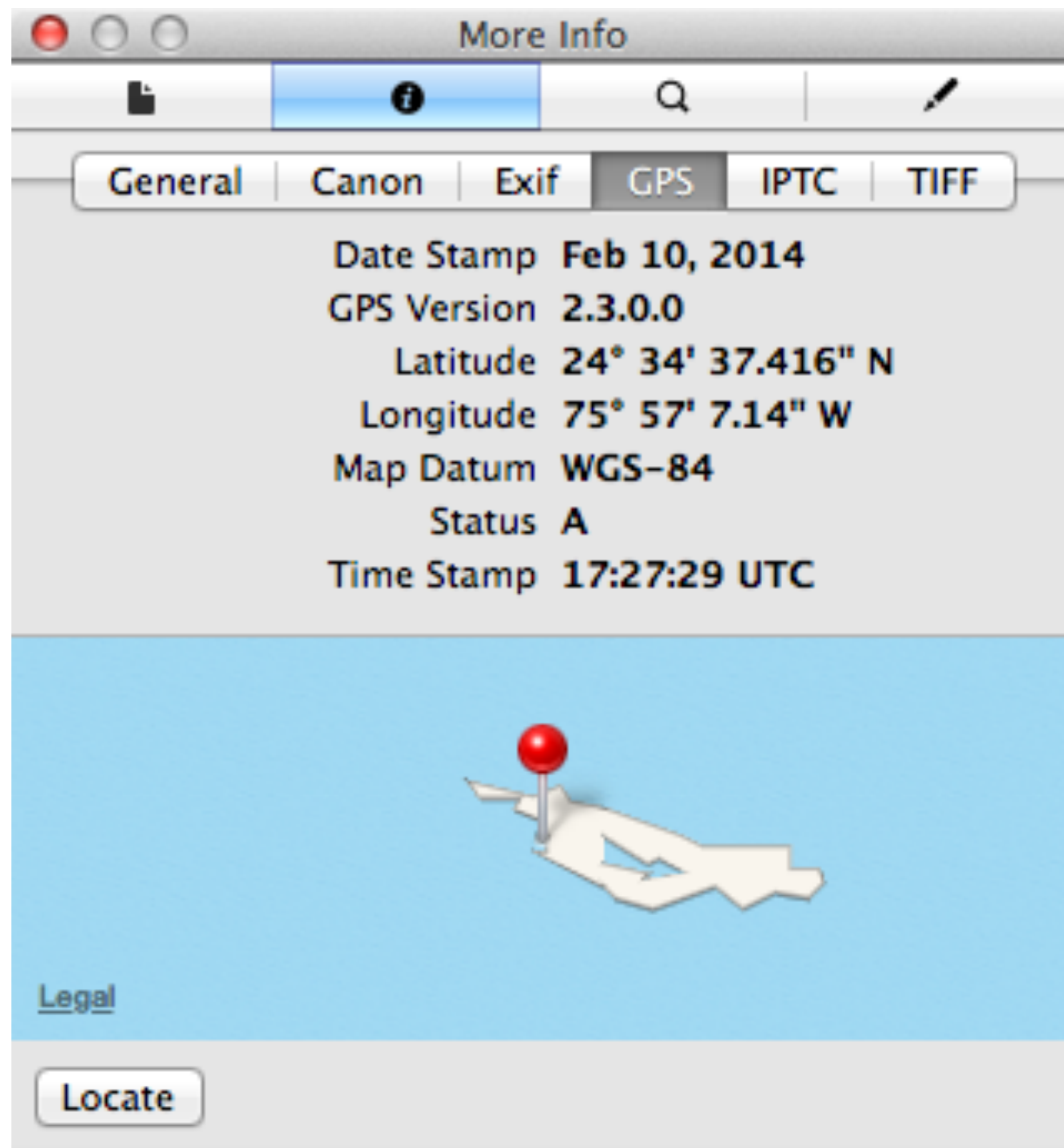
A photo also
contains
metadata — data
about the data

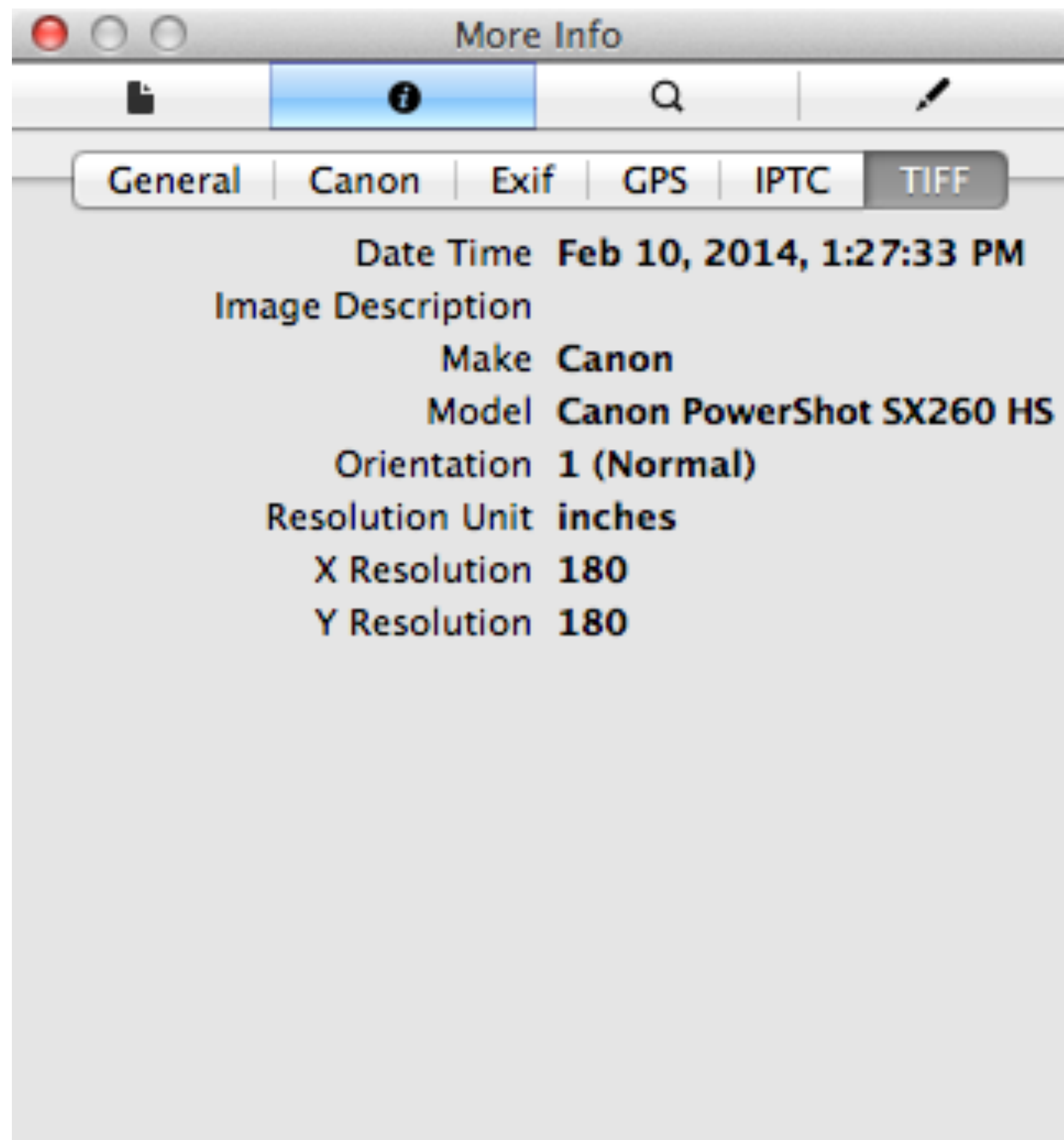












Metadata can tell you a ***lot***

For example:

- Metadata says you called the number of a telephone sex line
- ...at 2:31am
- ...and spoke for 47 minutes
- ...but they don't know what you spoke about.

For example:

- Metadata says you called the number of a suicide prevention hotline
- ...from the Golden Gate Bridge
- ...but they don't know what you spoke about.

For example:

- Metadata says you called the number of an HIV testing service
- ...and spoke for four minutes
- ...and then called your doctor's office
- ...and spoke for 27 minutes
- ...and then called your health insurance company
- ...and spoke for 81 minutes
- ...but they don't know what you spoke about.

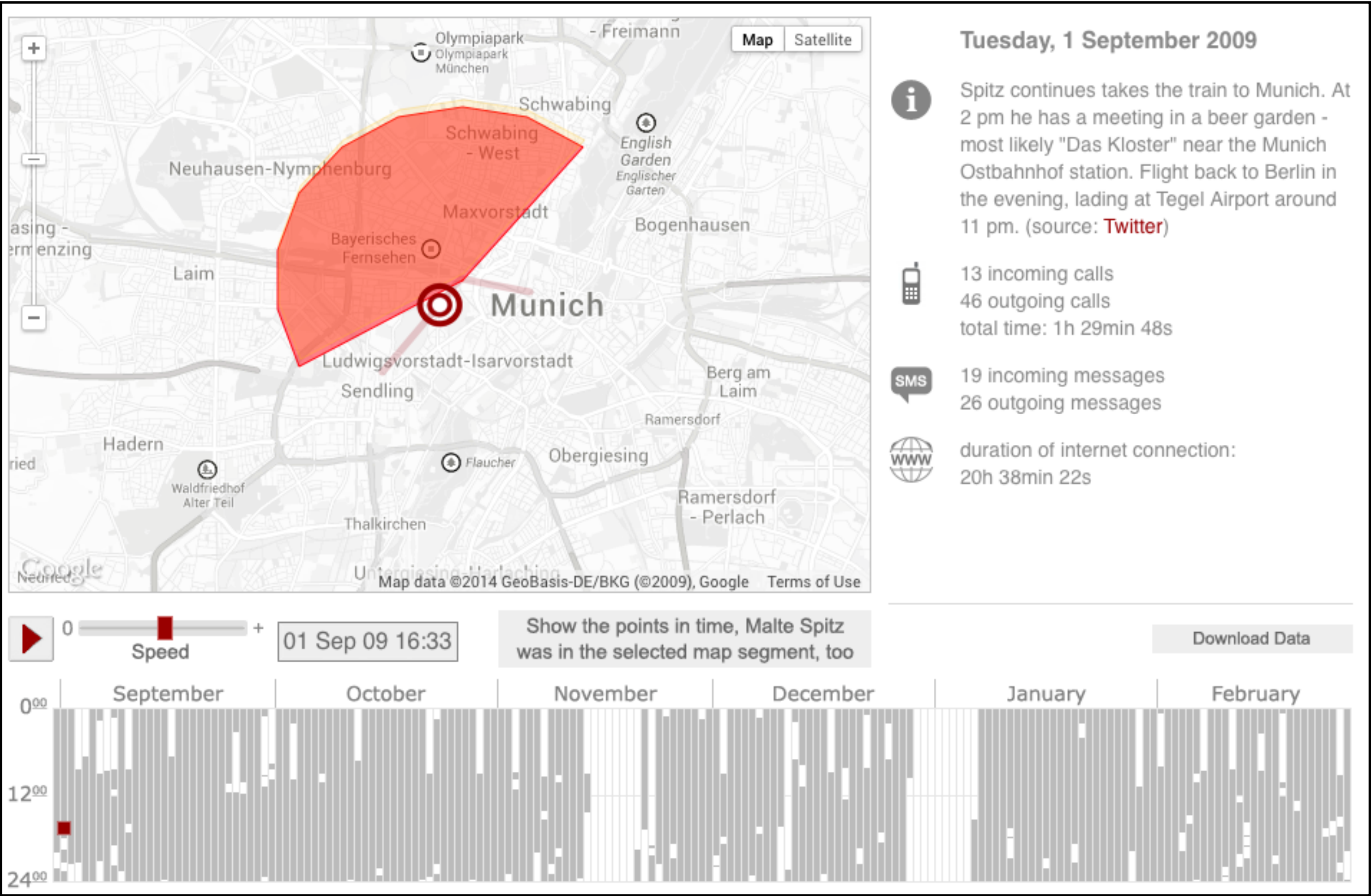
For example:

- Metadata says you received a call from the local NRA chapter office
- ...while they were having a legislation campaign against new gun laws
- ...and then you called the office of your US Representative
- ...and then sent them a Tweet
- ...but they don't know what you spoke about or what you wrote in the Tweet.

It's Only Metadata: Real-World Example

- German politician Malte Spitz sued to have the giant German telecom company Deutsche Telekom hand over six months of his phone data
- The German magazine *ZEIT Online* combined this geolocation data with information relating to his life as a politician, such as Twitter feeds, blog entries and websites, all of which is all freely available on the Internet.

Using only the DT cell phone “metadata,” combined with publicly-available information from the Internet, *ZEIT Online* reporters with no expert surveillance training or specialized surveillance tools, were able to re-construct a fairly detailed picture of Spitz’s week, minute-by-minute, as he worked, traveled, used the Internet and his cell phone, ate, slept and met with colleagues.





Kieran Healy

About · Publications ·
Teaching · Resources · Blog

Using Metadata to find Paul Revere

Sun Jun 9, 2013

London, 1772.

I have been asked by my superiors to give a brief demonstration of the surprising effectiveness of even the simplest techniques of the new-fangled *Social Network Analysis* in the pursuit of those who would seek to undermine the liberty enjoyed by His Majesty's subjects. This is in connection with the discussion of the role of "metadata" in [certain recent events](#) and the assurances of [various respectable parties](#) that the government was merely "sifting through this so-called metadata" and that the "information acquired does not include the content of any communications". I will show how we can use this "metadata" to find key persons involved in terrorist groups operating within the Colonies at the present time. I shall also endeavour to show how these methods work in what might be called a *relational* manner.

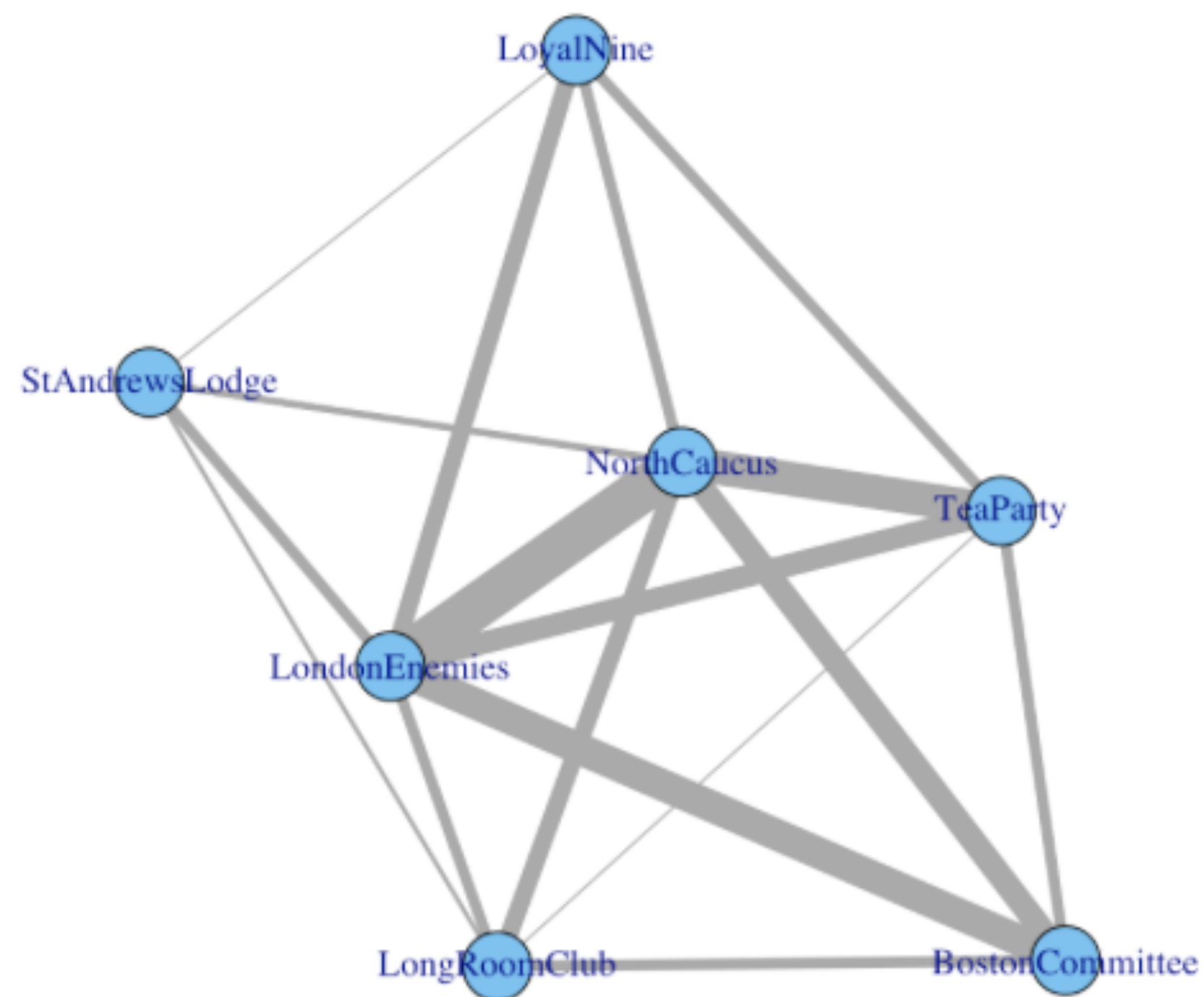
The analysis in this report is based on information gathered by our field agent Mr [David Hackett Fischer](#) and published in an Appendix to his [lengthy report to the government](#). As you may be aware, Mr Fischer is an expert and respected field Agent with a broad and deep knowledge of the colonies. I, on the other hand, have made my way from Ireland with just a



Kieran Healy

About · Publications ·
Teaching · Resources · Blog

Rather than relying on tables, we can make a picture of the relationship between the groups, using the number of shared members as an index of the strength of the link between the seditious groups. Here's what that looks like.

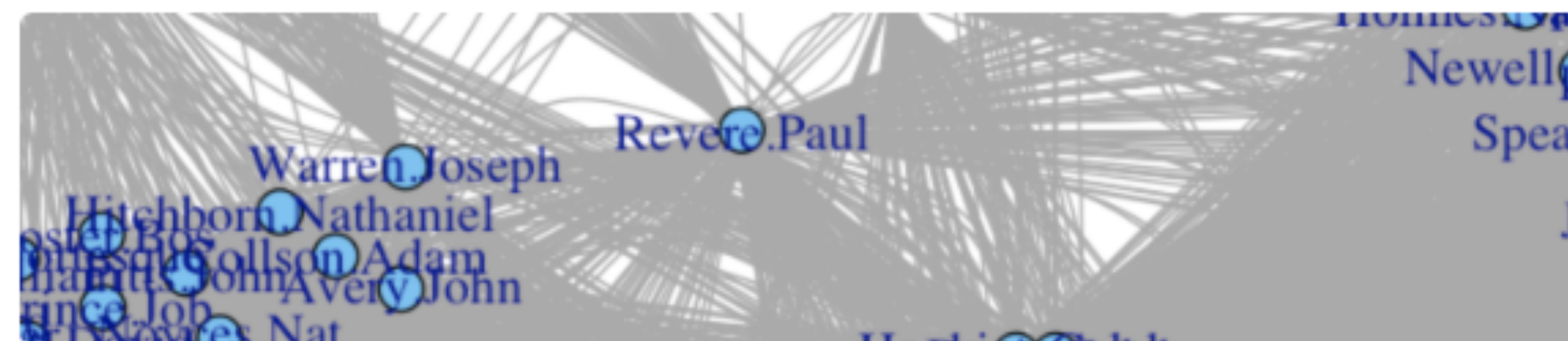




Kieran Healy

About · Publications ·
Teaching · Resources · Blog

What a nice picture! The analytical engine has arranged everyone neatly, picking out clusters of individuals and also showing both peripheral individuals and—more intriguingly—people who seem to bridge various groups in ways that might perhaps be relevant to national security. Look at that person right in the middle there. [Zoom in if you wish](#). He seems to bridge several groups in an unusual (though perhaps not unique) way. His name is Paul Revere.



Once again, I remind you that I know nothing of Mr Revere, or his conversations, or his habits or beliefs, his writings (if he has any) or his personal life. All I know is this bit of metadata, based on membership in some organizations. And yet my analytical engine, on the basis of absolutely the most elementary of operations in Social Network Analysis, seems to have picked him out of our 254 names as being of unusual interest. We do not have to stop here, with just a picture. Now that we have used our simple “Person by Event” table to generate a “Person by Person” matrix, we can do things like calculate centrality scores, or figure out whether there are cliques, or investigate other patterns. For example, we could calculate a [betweenness centrality](#) measure for everyone in our matrix, which is roughly the number of “shortest paths” between any two people in our network that pass

Hitchborn, Nathaniel
Bos, Collson, Adam
Harris, John, Avery, John
Gince, Job
Harris, Nat

Once again, I remind you that I know nothing of Mr Revere, or his conversations, or his habits or beliefs, his writings (if he has any) or his personal life. All I know is this bit of metadata, based on membership in some organizations. And yet my analytical engine, on the basis of absolutely the most elementary of operations in Social Network Analysis, seems to have picked him out of our 254 names as being of unusual interest. We do not have to stop here, with just a picture. Now that we have used our simple "Person by Event" table to generate a "Person by Person" matrix, we can do things like calculate centrality scores, or figure out whether there are cliques, or investigate other patterns. For example, we could calculate a [betweenness centrality](#).

Metadata Collection ***is***
Surveillance

“But if you aren’t doing anything wrong,
you should have nothing to hide!”

– An often-heard, but seriously flawed, defense of unchecked government surveillance

“Do you have curtains?”

“Can I look through your credit card statements for the past five years?”

“I don't have anything to hide, but I
don't have anything I feel like
showing you, either.”

Better answers

Privacy isn't necessarily, and is not usually, about hiding a wrong.

Privacy is a basic human right

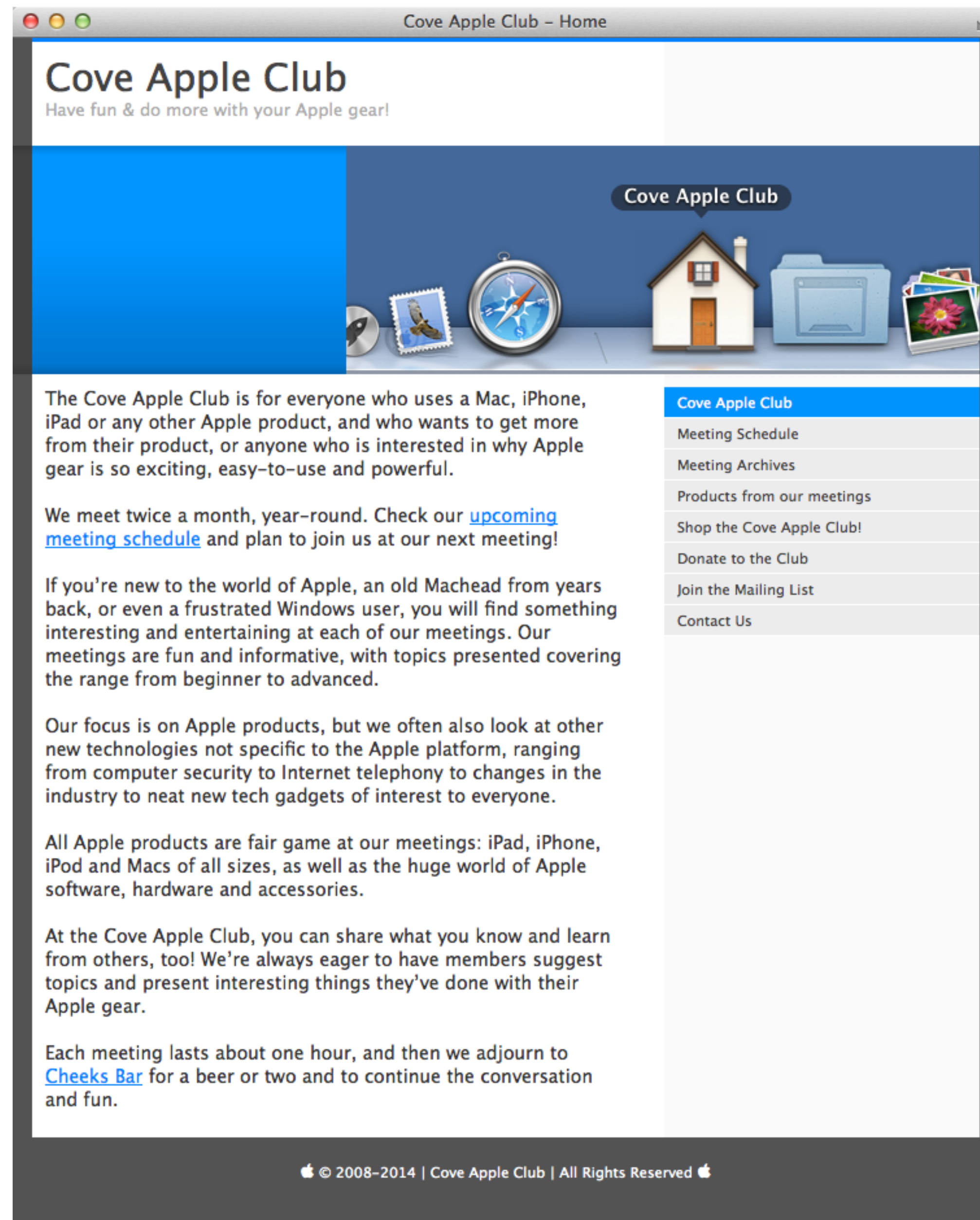
Surveillance can chill or inhibit basic rights such as free speech, free association or a free press.

The laws may change. What is legal
today may be illegal tomorrow.

But the basic premise is that we do not have to justify the protections that are ***guaranteed*** by the Fourth Amendment.

It's Only Metadata!

Your Clicks Pay for This Club



COVEAPPLECLUB.COM

Cove Apple Club

Have fun & do more with your Apple gear!

Cove Apple Club



The Cove Apple Club is for everyone who uses a Mac, iPhone, iPad or any other Apple product, and who wants to get more from their product, or anyone who is interested in why Apple gear is so exciting, easy-to-use and powerful.

We meet twice a month, year-round. Check our [upcoming meeting schedule](#) and plan to join us at our next meeting!

If you're new to the world of Apple, an old Machead from years back, or even a frustrated Windows user, you will find something interesting and entertaining at each of our meetings. Our

Cove Apple Club

Meeting Schedule

Meeting Archives

Products from our meetings

[Shop the Cove Apple Club!](#)

Donate to the Club

Join the Mailing List

Contact Us

Cove Apple Club

Have fun & do more with your Apple gear!

Cove Apple Club

The next time you need some new Mac gear, start your online shopping session with the link to Amazon on this page. Your purchase will earn a little money for the Cove Apple Club, which we save up all year for a big Holiday Party for all members of the club! We update club members on the earnings every month.

So be sure to click the Amazon logo below when you need to shop for Mac products online...and "give back" to the Cove Apple Club -- without costing you an extra cent! Thanks!

Shop earth's biggest selection

Books

Electronics

Video Games

HDTVs

Video On Demand

Kindle

DVD & Blu-ray

Smart phones

Netbooks

Desktops

MP3s

amazon.com

privacy information

On an iPhone or iPad? Amazon Banner above not displayed?
[Tap this link instead](#)

On a Mac? Make it even easier!
Just drag this link to your Bookmarks bar: [Amazon](#)

Need a Web site? Want your own email domain?

The Cove Apple Club **uses** and recommends [1&1 Internet](#). Unlimited hosting plans and personal email domains from \$0.99/month with 24/7 live telephone support.

1&1 MY WEBSITE

Cove Apple Club

Meeting Schedule

Meeting Archives

Products from our meetings

Shop the Cove Apple Club!

Donate to the Club

Join the Mailing List

Contact Us

© 2008–2014 | Cove Apple Club | All Rights Reserved

be sure to check the Amazon logo below when you need to shop for Mac products online...and "give back" to the Cove Apple Club -- without costing you an extra cent! Thanks!

[Donate to the Club](#)

[Join the Mailing List](#)

[Contact Us](#)



On an iPhone or iPad? Amazon Banner above not displayed?

[Tap this link instead](#)

On a Mac? Make it even easier!

Just drag this link to your Bookmarks bar: [Amazon](#)



Since Our Last Meeting

Earnings Report Totals

[Glossary](#)

February 11, 2014 to February 25, 2014


	Items Shipped	Revenue	Advertising Fees
Total Amazon.com Items Shipped	22	\$1,175.94	\$53.94
Total Third Party Items Shipped 	21	\$410.49	\$22.78
Total Items Shipped	43	\$1,586.43	\$76.72
Total Items Returned	0	\$0.00	\$0.00
Total Refunds	0	\$0.00	\$0.00
TOTAL ADVERTISING FEES	43	\$1,586.43	\$76.72

2014 Year-to-Date

Earnings Report Totals

[Glossary](#)

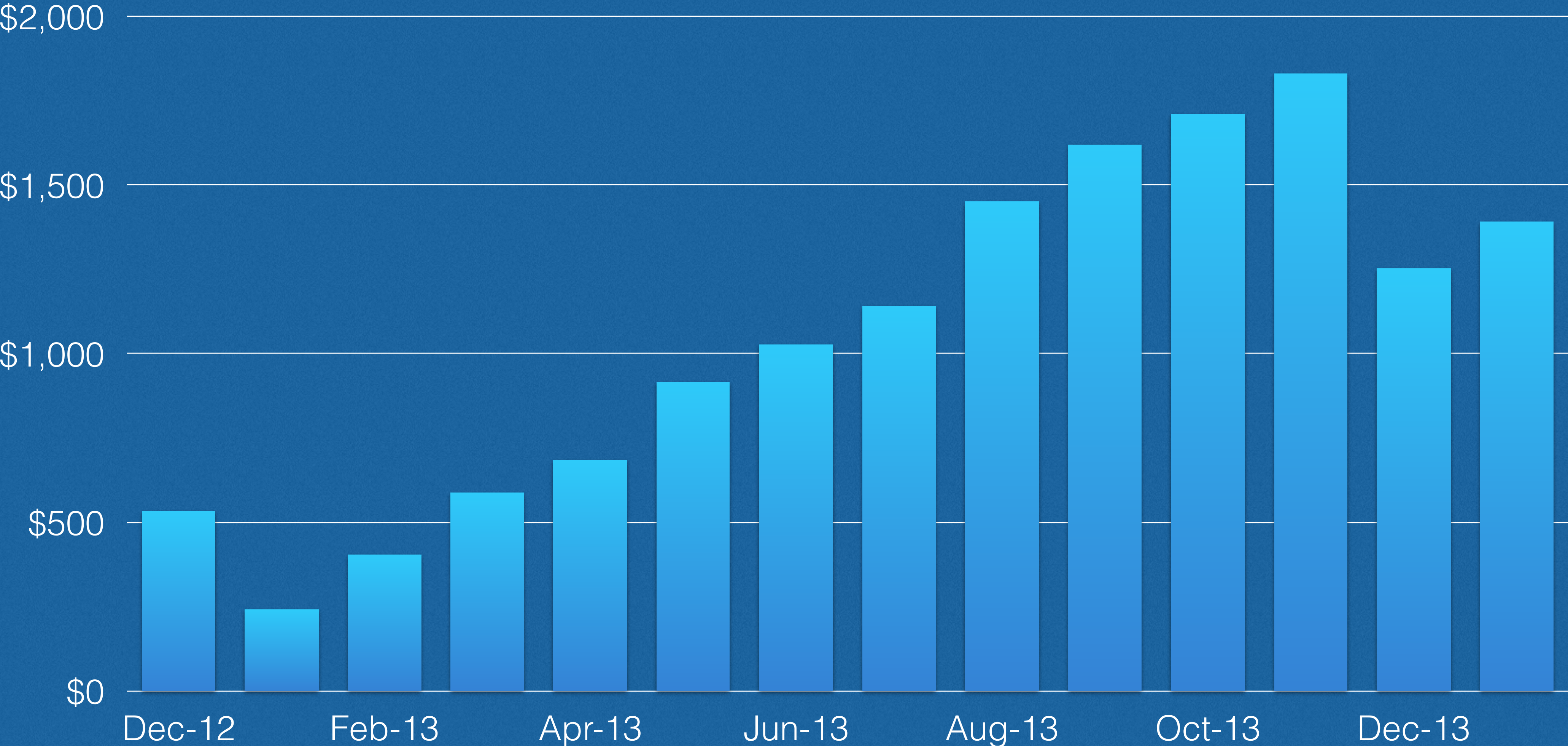
January 1, 2014 to February 25, 2014

	Items Shipped	Revenue	Advertising Fees
Total Amazon.com Items Shipped	131	\$4,091.96	\$169.84
Total Third Party Items Shipped 	99	\$2,179.05	\$126.45
Total Items Shipped	230	\$6,271.01	\$296.29
Total Items Returned	0	\$0.00	\$0.00
Total Refunds	0	\$0.00	\$0.00
TOTAL ADVERTISING FEES	230	\$6,271.01	\$296.29

Since Inception, October 2012

Earnings Report Totals Glossary			
January 1, 2012 to February 25, 2014			
	Items Shipped	Revenue	Advertising Fees
Total Amazon.com Items Shipped	868	\$44,812.02	\$1,982.71
Total Third Party Items Shipped 	977	\$19,537.51	\$1,157.49
Total Items Shipped	1845	\$64,349.53	\$3,140.20
Total Items Returned	-6	-\$315.21	-\$12.51
Total Refunds	0	\$0.00	\$0.00
TOTAL ADVERTISING FEES	1839	\$64,034.32	\$3,127.69

Cove Apple Club Bank Balance @ Month-End



Our Next Meeting

