Top 7 Gotcha’s That Can Shut Down Your Online Business
Top 7 Shocking Legal Gotcha’s That Can Shut Down Your Online Business…

And What to Do About It!

Chip Cooper, Esq.
Internet Attorney
Dedication

This book is dedicated to all Internet marketers and online entrepreneurs who’ve decided to adapt to the new legal environment on the Web, and who are determined to do it right!

To your everlasting success!

And…

To Cathy, my wife and partner for her support and love, and for many years of putting up with me!

Mission Statement

• To empower you with a Simple Online Legal Solution…

• so you can be as successful as you want, and to grow your online businesses, as fast as you want…

• with the confidence that you’re as legally protected as the Big Guys who can afford to hire expensive law firms,

• but without the high cost!
# Top 7 Gotcha’s That Can Shut Down Your Online Business

## Contents

<table>
<thead>
<tr>
<th>Gotcha</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Internet Landscape Has Changed!</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>What Does This Mean To You?</td>
<td>15</td>
</tr>
<tr>
<td>Gotcha 1</td>
<td>You Don’t Own Your Website, Software, And The Other Stuff You Outsourced!</td>
<td>25</td>
</tr>
<tr>
<td>Gotcha 2</td>
<td>Your Blog Blunders Create Huge Liability For Copyright Infringement</td>
<td>31</td>
</tr>
<tr>
<td>Gotcha 3</td>
<td>Your Membership Site Lands You On The FTC’s Top Target List</td>
<td>37</td>
</tr>
<tr>
<td>Gotcha 4</td>
<td>Your Ignorance Of Privacy-Protected Information Causes Massive FTC Fines</td>
<td>43</td>
</tr>
<tr>
<td>Gotcha 5</td>
<td>Your Own Privacy Policy Is Enforced</td>
<td></td>
</tr>
</tbody>
</table>
Top 7 Gotcha’s That Can Shut Down Your Online Business

Against You By The FTC
......................................................................................51

Gotcha 6
You Naively Rely Solely on Boilerplate Disclaimers To Protect You
...............................................................................................57

Gotcha 7
You Fall Into The FTC’s Biggest Trap By Unwittingly Collecting Privacy-Protected Information From U13’s
...............................................................................................67

What Are Your Options for A Real Legal Solution You Can Actually Have Confidence In?
...............................................................................................75

Conclusion
...............................................................................................85

Appendixes
Legal Gotcha’s That Didn’t Make The Top 7 List
...............................................................................................89

Appendix 1
FTC Accelerates Crackdown On Fake News Sites
...............................................................................................91

Appendix 2
Blockbuster FTC Settlement!

Jesse Willms Agrees To $359 Million
Top 7 Gotcha’s That Can Shut Down Your Online Business

Settlement For Deceptive Marketing Practice Claims
.................................................................................................................95

Appendix 3
FTC Liability Traps Internet Marketers
Must Avoid With Affiliate Marketers
.............................................................................................................101

Appendix 4
Why It’s Risky To Copy Stuff
Off The Web
.............................................................................................................107

Appendix 5
The FTC Begins Crackdown
On Behavioral Ads - Is Your Site
In The Cross Hairs?
.............................................................................................................111

Appendix 6
FTC's Settlement With Google Provides
Game Changing Internet Privacy Regulations
.............................................................................................................115

Appendix 7
Internet Marketers – Are You Liable For
Your Affiliates’ Trademark Infringement
With Sponsored Keyword Ads?
.............................................................................................................119

Appendix 8
3 CAN-SPAM Gotcha’s That Every
Internet Marketer Should Avoid
.............................................................................................................123
Appendix 9
If You’re Tempted To Use Fake Endorsements – Don’t Do It!
.................................................................................................129

Appendix 10
2 Legal Traps To Avoid When Writing Your Own Marketing Copy
.................................................................................................133

Appendix 11
Beware of Unintended Warranties If You Write Your Own Product Descriptions
.................................................................................................137

Appendix 12
Beware of Human Intervention With Online Contracting - 2 Costly Mistakes To Avoid
.................................................................................................141

Appendix 13
Do You Own - And Control Your Domain Name? You May Be Surprised!
.................................................................................................145

Appendix 14
Website Terms of Use: Are Yours Enforceable? Does It Matter?
.................................................................................................149

Appendix 15
3 Tips To Avoid Liability
For Actions of Your Online Resellers .................................................................153

Appendix 16
Are Non-Clickers Bound By Your Online Customer Agreement?
...........................................................................................................157

Appendix 17
Is Your Online Customer Agreement Enforceable Even against Simba, The Agreeable Cat?
...........................................................................................................161

Appendix 18
Sex, Lies... And a Dumb Mistake Your Blog Website Can’t Afford
...........................................................................................................165

Appendix 19
Your Online Customer Agreement - Which End-User Agreement Approach Is Right For You?
...........................................................................................................169

Appendix 20
How To Avoid FTC Biz Op Regulation ................................................................173

About Chip Cooper, Esq.
...........................................................................................................177
The Internet Landscape Has Changed!

The "Wild, Wild West" days of the Internet are over. It was fun while it lasted.

But make no mistake.

The legal landscape of the Internet has fundamentally shifted. You might not even have noticed...Yet.

The Federal Trade Commission (FTC) enforces the Rules and Regulations that govern unfair and deceptive marketing practices in the USA. If you don't know them, if you don't adhere to them, you do so at your own risk.

Plus, there are laws that are not new, but they’re not well known by most Internet marketers and online entrepreneurs. And they apply to your online business.

The scary thing is... these little known laws can have devastating effects if you don’t know how they apply to your online business. And know how to avoid their devastating consequences.

- Think ownership of your website, software and content.
• Think copyright infringement even if you didn’t actively participate in the infringing activity.

• Think massive FTC fines for unwittingly using deceptive marketing practices.

And that’s just for starters.

If you’ve been around for a while, you probably know that The “Wild, Wild West” ended in 2009. That’s when the tsunami of new laws and regulations affecting websites started.

During the “Wild, Wild, West” days, the buzz was about what color hat you were wearing as an Internet marketer or online entrepreneur.

• White Hat: you were completely ethical in your marketing practices.

• Black Hat: you used marketing practices that were considered by most to be unethical.

• Grey Hat: you used both White Hat practices and Black Hat marketing practices.

It’s vastly different now. And it’ll never be the same!

The color of your hat doesn’t mean much if the FTC comes knocking at your door!
What Does This Mean to You?

(Hint - You’d Better Adapt Now, or Risk Losing Your Business!)

It’s Not The Color of Your Hat Anymore!

For starters, it means that the color of your hat is just that… old hat!

Now, it’s about legal compliance (not your hat color). These are now the critical questions you must ask yourself:

- Is my website legal, and
- Are my marketing practices legal?

You’re Now on the FTC’s Radar 24 x7

And it also means that the Federal Trade Commission (FTC) is now on the warpath with new regulations and aggressive enforcement.

Just take a look at a few recent cases:
Top 7 Gotcha’s That Can Shut Down Your Online Business

- **$250,000** - 2011 - Learning Systems – affiliate marketers falsely posed as consumers & reviewers.

- **$500,000** - 2011 - 10 websites – fake news and consumer testimonials.

- **$350 Million** - 2012 - Jesse Willms – free offers and recurring billing plans.

- **$18 Million** – 2012 – Commerce Planet - free offers and recurring billing plan

One significant take-away from these cases and others is this: generally speaking, the marketing practices in these cases are the same marketing practices all Internet marketers and online entrepreneurs use:

- squeeze pages,
- testimonials for social proof,
- free offers,
- upsells,
- memberships and continuity plans, and
- and affiliate marketing partners.

The catch is that they were used *deceptively (and therefore illegally)*, according to the FTC, and therefore they became targets aggressively pursued by the FTC.

Sometimes, the deceptive practices were no-brainers, meaning they were clearly deceptive, and there’s no excuse or defense for these practices.

In other cases, however, the distinction was not as clear.
And in some, there were even legal agreements that disclosed material terms of offers, but the terms and conditions were not presented properly according to the FTC.

The result: huge fines, and other restrictions on future marketing practices.

**What is The FTC’s Legal Authority Anyway?**

In short, the FTC enacts consumer protection regulations. States have similar laws and regulations, but the primary focus is on the FTC.

The FTC was created by the U.S. Congress in 1914 for the purpose of protecting consumers against fraud.

Specifically, the FTC’s mission is to prevent “*unfair or deceptive acts or practices*”.

The FTC’s mission covers wide areas, including product warranties, product labeling and packaging, lending, fair credit billing and reporting and telemarketing. These areas, however, aren’t the ones that directly affect you.

The big areas that directly affect you and your lists are the FTC rules regarding privacy, data security, and online marketing practices, particularly:

- how you collect, use, and share information, and
- how you sell your products, services and information.
What Does The FTC Consider as “Deceptive” or “Unfair”?
In order to understand what the FTC believes is a “deceptive” or “unfair” act or practice, the best place to begin is with ad claims and business practices, because they are the key things the FTC focuses on.

**Tip:** In a nutshell, a *business practice* is a practice and/or procedure used by a business to achieve its goals.

**Tip:** In a nutshell, an *ad claim* is a statement regarding the performance, features and/or benefits of a product or service that is intended to persuade a consumer to respond favorably to a call to action. The call to action is what you want the prospect to do – sign up on your squeeze page, sign up for a webinar, provide information, take a survey, or purchase a product or service.

So, what makes an ad claim of business practice “deceptive” or “unfair” according to the FTC?

The FTC says that a claim is “deceptive” if it:

- is likely to mislead consumers acting reasonably under the circumstances; and
- is "material" - that is, important to a consumer's decision to buy or use the product or service.
The FTC says that a claim or business practice is “unfair” if it:

- causes or is likely to cause substantial consumer injury which a consumer could not reasonably avoid; and
- is not outweighed by the benefit to consumers.

These are the general principles followed by the FTC. They’re important only as beginning points.

**Tip:** What you really need to understand is how these principles are applied to the specific marketing practices you undertake every day.

**Tip:** And also, very important, is how you use your lists – specifically, how you use and share the personal information, and other privacy-protected information, in your lists.

How does the FTC determine if you’re engaged in “deceptive” or “unfair” practices?

- The FTC’s review focuses on what a reasonable consumer would think. Everything is considered – words, phrases, images, videos, slogans – to determine how a consumer would view what it conveys.
Top 7 Gotcha’s That Can Shut Down Your Online Business

- The FTC would consider what is stated and not stated. For example, what you actually say or do, and what is implied by what you say or do. You’re required to have substantiation (or proof) that you can back up your claims.

- Then the FTC considers if what you say and do would be material, or important, to a typical consumer regarding whether to act on your call to action.

How The FTC Can Shut Down Your Online Business

Engaging in “deceptive” claims or “unfair” practices can have massive consequences on your online business, your profits, and your family – and they’re all bad!

The FTC’s remedies include:

- Cease and desist orders – legally binding orders to stop the deceptive ad or practice.

- Corrective Ads – requirements to conduct new, corrective ad campaigns to correct the deceptive ad or unfair practice.

- Civil penalties – these can range from thousands to millions of dollars, and could wipe out your online business in a single day.

Tip – The FTC’s authority is very broad. The FTC can even freeze your bank and PayPal accounts!
The FTC’s Website Complaint Form

And here’s another take-away that you should be aware of.

This one’s big, very big. It could transform your life.

You probably know that the FTC has a website. What you may not know is that on this website they have a complaint form, and it’s really easy to find. All anyone has to do is to search online for “FTC Complaint” and it’ll show up as no. 1.

So, you now understand why it’s really easy for anyone with a complaint with the FTC - and all it takes is just one:

- a disgruntled customer,
- a privacy activist,
- your competitor…

To file a complaint against you that may very well transform you from being on the FTC radar (which all Internet marketers and online entrepreneurs are) – to being on the FTC’s target list.

Believe me, this is the last place you want to find yourself.

**Tip:** Don’t be fooled into thinking that you’re too small to be a target by the FTC. The FTC Complaint Form is available for anyone to file a complaint at any time.
And you should understand that even beginners are potential targets; it only takes a single disgruntled customer clicking on that FTC form to transform your life.

But it’s even more important to understand this - as you become successful, and grow your business, you’ll become even more of an *inviting potential target* for anyone who might want to file an FTC complaint or take some kind of legal action against you.

Now that the “Wild, Wild West” is over, a real, valid, honest-to-goodness *legal solution* is now just as essential, just as important, as your:

- shopping cart,
- email autoresponder, and
- email list.

**Personal Asset Protection Won’t Work Against The FTC**

Another thing… you may not realize it, but your personal assets are at risk. That’s right, your non-business assets and those of your family.

**Warning:** Regardless of how many legal entities you set up for purposes of personal asset protection, the FTC can go right through these barriers like a hot knife through butter.
Top 7 Gotcha’s That Can Shut Down Your Online Business

So, what to do?

First, you should focus on the Top 7 Legal Shocking Gotchas That Can Shut Down Your Online Business In a Single Day, and What to Do About It!

These are the BIG ONES – the really big mistakes and blunders - that you absolutely, positively need to understand and avoid.

At all costs!

There are some other Gotcha’s in the Appendixes. They are all important, but they didn’t make the cut for the Top 7 list.

**Tip:** Bottom line, if you’re serious about succeeding with your online business, you need to adapt to the new legal landscape on the Web. *Ignorance of the law is no excuse!*)
Top 7 Gotcha’s That Can Shut Down Your Online Business
Gotcha 1

You Don’t Own Your Website, Software, And The Other Stuff You Outsourced!

(Even Though You Paid For It!!)

What Could Be More Important Than Ownership?

The first Gotcha goes to the heart of your online business – ownership of your valuable intellectual property.

And it involves outsourcing – that is, hiring an independent contractor to develop valuable intellectual property for your business, such as:

- your website,
- your sales page,
- your software,
- your articles,
- etc.

These are all examples of what intellectual property attorneys call “copyrightable authorship”.
And if you’re like most Internet marketers and online entrepreneurs, you probably assume that if you pay the contractor to create this stuff, you own it. Right?

Wrong, in most cases in my experience in the trenches of my full-time Internet law practice. And here’s why.

The “Work Made For Hire Rules”

It’s all about the “work made for hire” rules of the U.S. Copyright Act.

Boiled down to its essence, here’s what the Copyright Act says:

- you will own the copyrights embodied in “copyrightable authorship”,
- created by your independent contractor (i.e. the person or entity who creates the work product),

only if all three of these elements are satisfied:

- there is a written “instrument” (typically an agreement or contract),
- that is signed by the independent contractor, and
- which provides that the work product is a “work made for hire”.

And if any of these three elements is not satisfied, your independent contractor owns the work product, by default.

And that’s the result… even if you pay for it, in full!
Tip: The default rules regarding “work made for hire” operate in favor of the outsourced contractor. For this reason, if you’re not diligent in protecting yourself, you lose!

All you get is a non-exclusive right to use the work product.

And it’s even questionable if you have rights to modify the work product.

Note: If you lose to the contractor in a “work made for hire” transaction, you lose more than copyright ownership. You also may lose competitive advantage with a competitor! Sit down for this one… the contractor, as owner, may license the work to anyone… even to your competitor!

You’d Be Surprised How Many Marketers Fall Into This Trap

You’d be surprised at how many Internet marketers and online entrepreneurs I see in my Internet law practice who are shocked to discover that they don’t own what they incorrectly assumed to be their valuable intellectual property.

And you’d be even more surprised at the cost in legal fees (and there’s no way to attach a value to the cost of
headaches and anxiety involved) for resolving messes regarding ownership.

It’s just so much easier to understand this Gotcha and to have the required legal documents.

For example, work made for hire clauses should be in your agreements with contractors, including:

- consulting agreements,
- development agreements, and
- services agreements.

And if you make the mistake of not providing for work made for hire at the beginning of your relationship with a contractor, you’ll need these agreements to “reel in” the copyrights:

- a copyright assignment, or
- a website ownership and transfer agreement.

So, now you have a better understanding of the old cliché - that ignorance of the law is no excuse!

Life is so much easier if you understand the basic legal rules, plus have the required legal tools and documents at your fingertips.

So, What Do You Do If You’ve Run Afool of Work Made For Hire?

So, how to reel ownership back in to you if your outsourcer owns work product because you didn’t follow the “work made for hire” rules?
The short answer is – you need to have the outsourcer sign a copyright assignment in your favor. This will have the effect of transferring the copyrights to you or your entity.

If your outsourcer has completed the work, and there will be no future contributions in the form of revisions or additions, then a straightforward copyright assignment will work.

However, if the outsourcer may make future revisions or additions, then you will need an additional clause transferring and assigning copyrights to these future works, to become effective automatically upon creation.
Gotcha 2

Your Blog Blunders Create Huge Liability For Copyright Infringement

You’re a Copyright Infringer Because of an Infringing Blog Post By Someone Else – And You Didn’t Even Know About It!

(That’s Right, You’re Technically Innocent, But Still Liable For Big Bucks!)

The Classic Situation

You’ve got a blog or forum on your website. After all, Google and other search engines love blogs, right?

And your blog or forum permits your website visitors to post comments.
Unknown to you, a person has stolen (copied without permission) an article from another website. This amounts to copyright infringement because the wrongdoer has exercised one of the exclusive rights of a copyright owner (the right to copy the work) without permission.

So far, there’s nothing surprising about this result.

But wait.

The visitor then posts the stolen (infringing) article on your blog or forum. The infringing article is now published on your blog or forum.

Now, it gets really surprising. Guess what… you’re also a copyright infringer!

Even if you have no knowledge!!

So, let’s recap. Even though you have no knowledge of the infringement and you’re technically innocent, you’re still liable as a copyright infringer.

And if the copyright owner can prove that you may have had knowledge, you could be nailed for statutory damages of up to $150,000 per work. Just imagine the pickle you would be in if there were multiple infringing works posted on your blog or forum.

This result may be surprising; however, attorneys understand that copyright infringement is a strict liability offense.

Not so, for the typical Internet marketer or online entrepreneur.
The DMCA Comes To The Rescue With The “Safe Harbor”

To remedy this problem for website operators, Congress passed the Digital Millennium Copyright Act (known as the “DMCA”) back in 1998.

The DMCA provides a so-called “safe harbor” from copyright infringement liability if:

- you provide a special DMCA notice in your Terms of Use, and
- you file a special DMCA Registration Form with the US Copyright Office.

Tip – Strict compliance with the DMCA rules is required to take advantage of the “safe harbor”.

Is the DMCA “Safe Harbor” Bullet Proof?

I am often asked… is the DMCA “safe harbor” bullet proof. In other words, are you completely safe as a website operator? No worries?

The short answer is… no, the DMCA “safe harbor” provides excellent protection for website operators, but it’s not bullet proof, according to the 2012 case, Viacom v. YouTube.

YouTube’s users, not by YouTube itself. YouTube defended based on its reliance on the DMCA “safe harbor”.

33
The District Court ruled in favor of YouTube in a motion for summary judgment, with the effect that YouTube was protected from infringement liability by the DMCA. The District Court found that since YouTube had insufficient knowledge of the infringing materials posted on its website, the DMCA “safe harbor” protected YouTube from liability.

The 2nd Circuit noted that there was evidence that YouTube may have had actual knowledge or awareness of infringing activity.

Internal YouTube emails indicated that videos of Bud Light commercials and CNN video clips were believed by YouTube management to be “blatantly illegal”, yet they were left on the YouTube site for a while in order to gain publicity for YouTube.

Based on this and similar evidence of YouTube’s actual knowledge or awareness of infringing activity, the 2nd Circuit held that a jury could find that YouTube was disqualified from the protections of the DMCA “safe harbor”.

As a result, the YouTube case was remanded back to the District Court to determine if there was sufficient evidence for a jury “to conclude that YouTube had the right and ability to control the infringing activity and received a financial benefit directly attributable to that activity.”
Tip – The DMCA “safe harbor” is not bullet proof. You need to be sure that you don’t have actual knowledge or awareness of infringing activity in order to take advantage of the “safe harbor”.

Gotcha 3

Your Membership Site Lands You On The FTC’s Top Target List

(Hint - Overlapping FTC & Little-Known State Regulations Now Make Continuity Programs The Most Regulated on the Web, and Penalties For Non-Compliance are Massive!!)

Warning! If you offer automatically renewed or continuous subscriptions for services in the United States, and specifically to California residents – including memberships, online or print content, or other subscription content – you’re now among the most regulated businesses on the planet!

Continuity or Negative Option Plans

Plans that offer automatically renewed or continuous
subscriptions for services have come under increased scrutiny and regulation from the U.S. Congress and the FTC. These plans are also described as:

- “continuity plans”, or
- “negative option plans”.

The key feature is that consumer charges are:

- automatically renewed, or
- continue periodically for an agreed upon time.

In a nutshell, the typical online businesses that are covered by these regulations are typically considered by Internet marketers and online entrepreneurs to be:

- membership sites, or
- subscription sites,
- this includes software-as-a-service (SaaS) sites as well.

**ROSCA**

In 2010, President Obama signed into law the Restore Online Shopper’s Confidence Act (ROSCA) which in part established three statutory rules for continuity programs:

- clearly and conspicuously disclose all material terms of the program prior to obtaining billing information (i.e. disclose the continuity program billing procedure prior to collecting credit card information),
Top 7 Gotcha’s That Can Shut Down Your Online Business

- obtain express informed consent before charging the consumer's account, and
- provide a simple mechanism for cancelling the plan.

The FTC was tasked with the responsibility of enforcement of ROSCA. Violations of ROSCA are treated as violations of FTC Act’s prohibition of unfair or deceptive marketing acts or practices.

**Nominal-Fee-To-Pay Offers**

Since its enactment, the FTC has been active in enforcement of ROSCA. Two recent cases sent the message of aggressive FTC enforcement loud and clear: one for a settlement of $359 million and another was litigated for a verdict of $18 million.

Both of these cases involved what are generally known as “nominal-fee-to-pay offers”, meaning that the consumer is lured into a continuity program with a an offer at a nominal charge (typically only a shipping and handling charge to get the customer’s credit card information).

With a “nominal-fee-to-pay offer, the initial offer is:

- followed up with an upsell to a free trial, and
- when the free trial period expires, the consumer’s card is then charged periodically until the consumer cancels.
Tip – One of the takeaways of these cases involving “nominal-fee-to-pay offers” is that the call to action for the nominal fee offer should have also provided the required ROSCA disclosures.

The FTC made it clear that even if the consumer is informed later (after the consumer accepts the nominal fee offer); it’s a deceptive practice if you don’t provide the ROSCA disclosures at the time of the call to action for the nominal fee offer.

**California False Advertising Act – SB 340**

The SB 340 amendments to the California False Advertising Act add these requirements for offers of automatically renewed or continuous subscriptions for services:

- a clear and conspicuous display of written terms (not a link) in visual proximity to the request for consent;

- an acknowledgement of renewal terms, cancellation policy, and how to cancel; and

- a clear and conspicuous notice of material changes and how to cancel.

Some of these requirements overlap with the ROSCA requirements, and some do not.
Compliance With Both ROSCA And SB 340

The real question is – how to comply both with ROSCA and SB 340 if you have a membership site, subscription site, or a SaaS site?

The following steps are recommended:

- **Offer terms:** the offer terms should be provided in written form (not a link), and should be separated by the size, type, or color of surrounding text; for visual proximity, place them above the call to action; all of the above should be prior to collecting billing information.

- **Express, informed consent:** after presentation of the offer terms, but before charging the customer’s account, require the customer to click on an I AGREE button.

- **Email acknowledgement:** after the customer has given express, informed consent, email an acknowledgement of the consent to the customer; the acknowledgement email should provide the offer terms, cancellation policy, and information regarding how to cancel; recommend that the customer retain the email for future reference.

- **Cancellation mechanism:** the cancellation mechanism should be simple and easy to use.

- **Notice of modifications:** if there are changes to the terms of the offer, email the customer with a clear email heading providing easily understandable
information in detail regarding the changes and how to cancel.

Note – If you offer a continuity plan – essentially, any plan for automatically renewed or continuous subscriptions for services to California residents – including memberships, online or print content, or other subscription content, you’re now required to comply with two sets of regulations – one for ROSCA and another for the California False Advertising Act (SB 340).

Violations Can Result in Huge Fines

The consequences for violations of ROSCA and California SB 340 are huge:

- FTC sanctions for ROSCA violations of up to $16,000 PER VIOLATION!
- California sanctions of $2,500 PER VIOLATION!
Gotcha 4

Your Ignorance Of Privacy-Protected Information Causes Massive FTC Fines

You Don't Know What Information Is Privacy-Protected & What To Do About It!

(Hint – Social Media And Mobile Apps Are Huge Traps For the Unwary!!)

Background

You’re an online entrepreneur, or maybe you even view yourself as an “IM”, and Internet marketer - a special breed of cat that’s a subset of online entrepreneurs.

In either case, it doesn’t matter if you’re a veteran or a beginner. It doesn’t even matter if you work in a home office, or in a real, brick and mortar office. You know one important, overriding thing.
And that’s the value of your email marketing list. The holy grail of online marketing.

With a responsive email list, you can grow your business. You can market additional products, services, or information you might create in the future.

Or, you may market complimentary stuff of others – your JV partners.

You’ve known from day 1 that the single greatest asset of your growing online business is your email marketing list. That’s why you expend so much time and effort growing it.

What you probably don’t know is this – it’s what I call the “great paradox”. The fact that your most valuable asset is also your single greatest source of legal liability. Massive liability that could shut your business down in a single day.

This critical fact has been known by Internet attorneys like me for some time. But among online entrepreneurs and IM’s, not very much at all.

And this is a huge problem if you continue to focus solely on building your list - at the expense of caring for it and protecting yourself as you grow and use it.

Tip – You absolutely, positively need to pay more attention to protecting your email list and yourself. And that begins with understanding what information is privacy-protected!
How Privacy Regulation Began in the United States

Certain information is privacy-protected. It’s protected so much by the FTC that it’s almost viewed as sacred. And this is the basis for all legal regulations that affect your list.

The best way to get a perspective on privacy-protected information is to understand how privacy regulation began in the United States.

It all started back in 2004 in California, not in the U.S. Congress. The California Online Privacy Protection Act (OPPA) became effective on July 1, 2004.

OPPA requires website operators who collect online “personally identifiable information” from California residents to post a Privacy Policy on their websites. So, at the time of the beginning of formal privacy protection in the U.S. privacy-protected information was limited to “personally identifiable information” which included:

- first name, last name,
- street address,
- email address,
- phone number, and
- social security number

In addition, privacy-protected information included other information if linked to any of the above elements of “personally identifiable information” such as:

- height
- weight
• occupation
• birth date
• etc.

After OPPA went into effect, websites selling the products into the United States began to post Privacy Policies that were OPPA-compliant. This was the result for two basic reasons:

• it would have been difficult to screen out California residents with confidence, and

• who among Internet marketers and online entrepreneurs would want to screen out California residents anyway, since California is such a large market.

So, in essence, OPPA became a de facto federal statute of general application, meaning that it applied the general market, and was not restricted in application to specific markets.

There are federal statutes that protect privacy of specific information (as distinguished from statutes of general application such as OPPA. A few of these are:

• Health Insurance Portability and Accountability Act of 1996 (HIPAA) for patient health records,

• Gramm-Leach-Bliley Act (GLBA) for financial information,
- Children’s Online Privacy Protection Act (COPPA) for personal information of children under age 13, and,
- Fair Credit Reporting Act (FCRA) for data collected by consumer reporting agencies.

Note – To this day, however, California’s OPPA statute is the only privacy statute of general application in the U.S. The FTC regulates privacy under the general principles of Section 5 of the FTC Act. For more information regarding the FTC’s authority, see the Chapter titled “What Does This Mean to You”.

Social Media-Related Additions To Privacy-Protected Information

One big headache for Internet marketers and online entrepreneurs is that privacy-protected information is a moving target, meaning that it changes from time to time, as new technology leads to new privacy concerns.

Warning! – Because privacy-protection information is in a constant state of evolution, marketers must remain vigilant for new additions, or risk huge fines for non-compliance with ever-expanding privacy regulations.

For example, perceived abuses regarding social media caused the FTC to expand the scope of privacy-protected
On March 20, 2011, the FTC announced its proposed settlement regarding Google's social media online service known as “BUZZ”.

In the proposed settlement, the FTC added new categories of privacy-protected information, which include:

- Physical location data,
- Screen names, and
- Lists of contacts.

Tip – Beginning with the Google settlement on March 20, 2011, marketers must treat physical location data, screen names, and lists of contacts as privacy-protected information.

Mobile App-Related Privacy Rules

Both the State of California and the FTC have moved to regulate the booming market for mobile phone applications known as “apps”.

Privacy concerns were heightened as a result of several incidents involving mobile phones, including:

- A blogger discovered that a social network app had uploaded his mobile phone contacts without permission,
On February 22, 2012, the California Attorney General announced that the California Online Privacy Protection Act (OPPA) applies not only to protected information collected through websites, but also via apps on mobile devices.

The result: mobile apps that collect privacy-protected information, including physical location data, from California residents should have a Privacy Policy just as websites do.

Shortly thereafter in August, 2012, the FTC jumped on the mobile app privacy bandwagon by announcing in its report titled “Marketing Your Mobile App – Get it Right From The Start” that, among other requirements, mobile app publishers should:

- get express, affirmative consent before collecting sensitive data such as “geo-location”, medical, or financial data, and

- obtain verified parental consent before collecting personal information from children under 13 (U-13’s).
Tip – Social media and mobile apps are just the latest developments that trigger new privacy regulations. New regulations will be coming down the pike at an increasing rate. Keep up and comply with them, or suffer huge headaches and massive fines!

**What to Do About Your Collection And Use of Protected Information**

Once you know what information is privacy-protected, it’s critical that you know what to do about it in terms of disclosures in your Privacy Policy.

In general terms, your Privacy Policy, regardless of whether it is posted on your website or via your mobile app, should disclose the following:

- the dates that the Privacy Policy takes effect,
- the categories of privacy-protection information collected,
- how privacy-protected information is collected,
- how users may change privacy-protected information,
- the process for notification regarding changes to the Privacy Policy, and
- how privacy-protected information is shared or made accessible to others, particularly for marketing purposes.
Gotcha 5

Your Own Privacy Policy Is Enforced Against You By The FTC

You Don’t Do What You Say or Do What You Say You Won’t in Your Privacy Policy!

(Hint - You Mistakenly Believe That Your Boilerplate Privacy Policy Will Protect You!!)

Background

The FTC, in its August, 2012 report titled “Marketing Your Mobile App – Get it Right From The Start” put it this way regarding mobile apps, but it reflects the FTC’s policy generally:

“Honor your privacy promises. ‘But we don’t make any promises.’ Think again and reread your privacy policy or what you say about your privacy settings. Chances are you make assurances to users about the security standards you
apply or what you do with their personal information. At
minimum, app developers – like all other marketers – have
to live up to those promises. The FTC has taken action
against dozens of companies that claimed to safeguard the
privacy or security of users’ information, but didn’t live up
to their promises in the day-to-day operation of their
business. The FTC also has taken action against businesses
that made broad statements about their privacy practices,
but then failed to disclose the extent to which they collected
or shared information with others – like advertisers or other
app developers.”

The FTC treats the statements in your Privacy Policy just as
it would treat your ad claims for purposes of “deceptive”
practices.

As discussed in the first chapter titled “The Internet
Landscape Has Changed!” FTC says that an ad claim is
deceptive if it:

• Is likely to mislead consumers acting reasonably
under the circumstances; and
• Is "material" - that is, important to a consumer's
decision to buy or use the product or service?

So, this logically leads to the Cardinal Rule that the FTC
expects you to follow:

Cardinal Rule – Regarding your Privacy Policy, be sure to
do what you say and don’t do what you say you won’t. If
you violate this Cardinal Rule, you will be liable for an
FTC claim for “deceptive” practices!
Examples of Cardinal Rule Violations Taken From Actual FTC Cases

- The FTC Settlement With Google – In 2011, the FTC settled claims with Google regarding alleged “deceptive” practices involving Google’s BUZZ service. The FTC pointed to Google’s Privacy Policy which stated: “When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use.” The FTC alleged that Google violated this promise when Google by shifting Gmail users to its new BUZZ service without permission.

- The FTC Settlement With Chitka – Also in 2011, the FTC settled claims with Chitka regarding alleged “deceptive practices involving the passing of cookies to consumers. The FTC pointed to Chitka’s Privacy Policy which promised that consumers could opt out of having cookies passed to their browsers. The FTC alleged that Chitka violated this promise when the opt out lasted only 10 days.

- The FTC Settlement With Twitter – In 2010, the FTC settled claims against Twitter involving data security lapses that permitted two hackers to access users accounts. The FTC pointed to Twitter’s Privacy Policy which stated: “We employ administrative, physical, and electronic measures designed to protect your information from
unauthorized access.” The FTC alleged that Twitter violated this promise by using weak passwords that used lowercase, common dictionary words.

**Don’t Shoot Yourself in the Foot With Careless and Overbroad Statements**

If you apply the rules regarding “deceptive” ad claims, you can see why certain statements you may make in your Privacy Policy and squeeze pages, and easily be construed as “deceptive”, depending on how they are worded.

The result – you’ve unwittingly shot yourself in the foot!

For example, consider this classic statement: WE WILL NEVER SELL OR RENT YOUR PERSONAL INFORMATION. “Never” means exactly that – never!

Now thinks this through. Let’s parse the statement. Isn’t it likely that you may sell your online business or website in the future? And isn’t it likely that you may share protected information with JV partners and resellers? If you do, you’d be in violation of your promise.

And wouldn’t this promise be material to your list? Of course it would!

So, the promise with the term “never” is at least deceptive, and probably not true on its face. You should always be wary of absolute statements regarding use and sharing of protected information.
A better approach would be to change the statement to read (assuming it's true) to:

• **WE WILL NEVER SELL OR RENT YOUR PERSONAL INFORMATION FOR DIRECT MARKETING PURPOSES,** or

• **WE WILL NEVER SELL OR RENT YOUR PERSONAL INFORMATION WITHOUT YOUR PRIOR OPT-IN CONSENT.**

Tip – Avoid making absolute statements regarding your use and sharing of protected information.

Another area where it’s easy to make a statement that’s deceptive is with outlandish claims for data security.

For example, **WE PROTECT YOUR INFORMATION WITH THE HIGHEST INDUSTRY STANDARDS FOR DATA SECURITY.**
Again, let’s parse the statement. What are the HIGHEST industry standards for data security? Does HIGHEST mean military grade security? Does it mean compliance with ISO standards?

You may always deliver extremely high levels of data security; however, you’re way better off to promise no more than what the FTC requires - WE WILL PROVIDE REASONABLE AND ADEQUATE SECURITY …

Tip – Boilerplate Privacy Policies usually don’t protect you because they make “standard” privacy statements that may not apply to you, and in many cases they fail to make statements that you should make regarding your actual marketing practices involving the collection, use, and sharing of privacy-protected information. For this reason, it’s always recommended that you have a Privacy Policy that’s tailored to your specific marketing practices.
Gotcha 6

You Naively Rely Solely on Boilerplate Disclaimers To Protect You

You Fail To Cover Your Bases With Special Legal Disclaimers

(And You Don’t Understand The FTC Rules For Earnings Disclaimers And “Success Story” Testimonials!!)

Boilerplate Disclaimers

OK, so what’s a boilerplate disclaimer?

This is a classic example:

DISCLAIMER.

ALL GOODS, PRODUCTS, SERVICES,
INFORMATION, CONTENT, AND/OR MATERIALS AVAILABLE ON THIS SITE, ARE PROVIDED ON AN "AS IS" BASIS WITH ALL FAULTS.

THE OWNER AND ITS AFFILIATES AND CONTENT PROVIDERS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, AND HEREBY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT RELATING TO THE GOODS, PRODUCTS, SERVICES, INFORMATION, CONTENT, AND/OR MATERIALS AVAILABLE ON THIS SITE, THE OPERATION OF THE SOFTWARE ON THIS SITE, AND THE TRANSACTIONS PERFORMED ON THIS SITE.

WITHOUT LIMITING THE FOREGOING, THE OWNER AND ITS AFFILIATES AND CONTENT PROVIDERS MAKE NO REPRESENTATIONS OR WARRANTIES THAT THE GOODS, PRODUCTS, SERVICES, INFORMATION, CONTENT, AND/OR MATERIALS AVAILABLE ON THIS SITE (i) WILL MEET YOUR REQUIREMENTS, (ii) WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE, (iii) WILL BE ACCURATE OR RELIABLE, (iv) WILL BE COMPLETE OR AVAILABLE, OR (v) WILL MEET YOUR EXPECTATIONS.

YOU ASSUME THE ENTIRE RISK OF SELECTION AND USE OF THE TRANSACTIONS PERFORMED ON THIS SITE, AND THE GOODS, PRODUCTS, SERVICES, INFORMATION, CONTENT, AND/OR MATERIALS AVAILABLE ON THIS SITE.
The purpose of the boilerplate disclaimer is to disclaim, in a general way, all warranties for anything and everything available on your website.

Warning! – Boilerplate disclaimers may not be effective for certain special situations and circumstances. That’s where special disclaimers come into play.

Special Disclaimers (Think Earnings Disclaimer)

The classic example of a special disclaimer that Internet marketers who sell products, services or information relating to how to make money on the Internet is the Earnings Disclaimer.

The typical Earnings Disclaimer:

- Disclaims assurance, representations, or promises regarding future earnings or income
- Disclaims any representation of making any specific amount of money or any money at all
- Disclaims any representation that there will be no loss of money
- Disclaims any prior success or results as an indicator of future success or results
- Disclaims any representation regarding suitability
- Describes applicable risk factors
- Recommends that qualified professionals assist with an evaluation of any business opportunity
Most Internet marketers and online entrepreneurs understand the need for an Earnings Disclaimer, and most have one that is effective at least to some degree.

However, there are other special situations and circumstances that require a special disclaimer, and if you fail to cover your bases, you may very well be liable for huge damages.

Here are a few examples:

- Disclaimer By Website Developer - No Responsibility For Website Legal Compliance
- Subjective Subject Matter Disclaimer
- Subjective Subject Matter Disclaimer - 3rd Party
- Disclaimer – Blog Posts by Others
- Disclaimer – No Investment Recommendations
- Disclaimer – Investment in Penny Stocks
- Disclaimer – No Obligation/Tax Prep Software
- Disclaimer – No Legal Representation
- Disclaimer – Information Not a Consumer Report
- Disclaimer – Licensing For Auctions
- Disclaimer – Diets/Restaurants Recommendations
- Disclaimer – Health and Rehabilitation
- Disclaimer – Exercise Routine
- Disclaimer – Diet Program
- Disclaimer – Dietary Supplements
Pitfalls To Avoid With Earnings Disclaimers

Effective on March 1, 2012, the FTC’s new Business Opportunity Rule (New Biz Op Rule) became effective.

The Biz Op Rule applies to a specific type of offer defined as a “Business Opportunity” (Biz Op).

The FTC’s objective with the New Biz Op rule was to make it very tough to make legally compliant Biz Op offers, particularly Biz Op offers that make earnings claims.

Warning! – Because the New Biz Op Rule imposes numerous, detailed requirements, Internet marketers and online entrepreneurs should not offer Biz Ops. Even with careful attention to all the requirements, it would still be relatively easy to inadvertently cross the line into non-compliance. In a nutshell, offering Biz Ops is a very high risk activity that should be avoided altogether. See Appendix 20 for information regarding how to avoid FTC regulation under the New Biz Op Rule.

What is an earnings claim under the New Biz Op Rule? The FTC defines an earnings claim as:

“…any oral, written, or visual representation to a prospective business opportunity purchaser which states a specific level of potential sales, income, gross or net profit for that prospective business opportunity purchaser, or which states other facts which suggest such a specific level”.
Here are a few examples of earnings claims:

- a statement that the purchaser could earn a “six figure income”;
- a photo of purchaser standing beside a luxury automobile (suggesting that earnings at a level that could afford such an automobile);
- a statement that “you could easily earn back your investment”; and
- screen shots of a PayPal account showing revenues earned.

If you’re offering a Biz Op and you make an earnings claim, the New Biz Op Rule imposes so many disclosure and substantiation requirements that it’s almost impossible to have confidence that you comply, even if you make a concerted effort.

You might ask: if you’re not offering a Biz Op, then the earnings claim disclosure and substantiation rules don’t apply, right?

The answer: technically “Yes”. However, you need to understand that:

- the FTC strongly dislikes earnings claims because the likelihood of deception is high, and
- the rules that apply to Biz Ops regarding earnings claims are a clear indication of where the FTC is headed with future enforcement.

So, if you make any earnings claims, it’s highly recommended that you follow these rules:
Top 7 Gotcha’s That Can Shut Down Your Online Business

- your claim should be relevant to the geographic market in which the opportunity is to be located;
- you have a reasonable basis for your claim;
- you have written material that supports your claim; and
- you make this material available to persons to whom you make the offer.

Warning! Don’t make an earnings claim and then post an Earnings Disclaimer. This would definitely be a violation of the New Biz Op Rule. In addition, it is highly likely that the FTC would view it as a deceptive practice, even if you aren’t regulated under the New Biz Op Rule. Think about it – you flagrantly make earnings claims, but your Earnings Disclaimer says you don’t. At the very least, it’s confusing. At worst, it’s deceptive!

New Rule Regarding “Success Story” Disclaimers

Warning! – Most Internet marketers and online entrepreneurs are not aware of the new rule regarding “success story” disclaimers. Failure to follow the new rule could lead to huge deceptive practice claims by the FTC.

“Success story” testimonials have long been a staple for advertisers with their website legal forms. “I lost 12 pounds in my first month… “ and “In 3 short months I was
taking in over $5,000 per month on my website…” are
typical examples.

The FTC in its *Guides Concerning the Use of Endorsements and Testimonials in Advertising* (16 C.F.R., Part 255) effective in December, 2009 placed severe restrictions on the use of the “results not typical” special disclaimers with “success story” testimonials, and failure to comply could result in significant legal liability.

**The Old “Results Not Typical” Disclaimer**

Prior to the latest Guides:

- websites could post “success story” testimonials that were not what most consumers would generally expect to achieve if they also provided a conspicuous “results not typical” disclaimer, and

- the “results not typical” disclaimer was considered a “safe harbor” shielding advertisers from liability for deceptive advertising.

The underlying theory was that the “results not typical” website legal forms disclaimer was sufficient to inform consumers about how unusual are atypical the advertised results might be. The latest Guides reflect the new belief by the FTC that “disclaimers of typicality” are not sufficient notices to consumers in most cases.

**The FTC Eliminates The “Results Not Typical” Disclaimer?**

Prior to issuing the latest Guides, the FTC conducted two consumer research studies that concluded that most
Top 7 Gotcha’s That Can Shut Down Your Online Business

consumers would interpret “success story” testimonials as being representative of what most consumers could expect to achieve. Relying on these studies, the FTC changed its posture regarding the “results not typical” disclaimer that accompanies “success story” testimonials.

Under the latest Guides, the FTC eliminated the prior “safe harbor” for the “results not typical” disclaimer.

New Rule – Now, advertisements that feature a consumer who provides an endorsement featuring his or her experience with a product or service as typical when that is not the case will be required to clearly disclose the results that consumers can generally expect to achieve from the advertised product or service.

In addition, if you disclose the results that consumers can generally expect to achieve, you must have clinical data to substantiate your claim.

This is how the FTC put it: "If the advertiser does not have substantiation that the endorser's experience is representative of what consumers will generally achieve, the advertisement should clearly and conspicuously disclose the generally expected performance in the depicted circumstances, and the advertiser must possess and rely on adequate substantiation for that representation."

For example, if you post a testimonial from John Doe that says he lost over 100 pounds in a year eating your low-fat yogurt when combined with an exercise program, you must
disclose the typical experience most consumers should expect, such as – “most consumers who eat our yogurt and also exercise regularly should not expect to lose over 100 pounds in a year; instead they should expect to lose only 10-15 pounds”). And, you must also be able to substantiate the 10-15 pound claim.

Note – The FTC did not completely shut the door on the “results not typical” disclaimer. The FTC did not state that typicality disclaimers would always be insufficient notice to consumers; however, it’s clear that the “results not typical” disclaimer has been drastically diminished, if not effectively eliminated.
Gotcha 7

You Fall Into The FTC’s Biggest Trap By Unwittingly Collecting Privacy-Protected Information From U13's

(Hint – Music, Games, Contests, Ads or Plug-Ins That “Could” Be Attractive To Children May Put You At the Top of the FTC’s Hit List!!)

If protection and security privacy-protected information is sacred to the FTC, then the collection of privacy-protected information from children under the age of 13 (U13s) is ultra-sacred.

The Children's Online Privacy Protection Act (COPPA) prohibits the collection, use, or disclosure of personal information from U13s on the Internet through the use of unfair or deceptive practices.
COPPA requires parental notification and consent prior to the collection of such information, and as you'll see below, COPPA applies not only to sites that target U13s, but also to general audience sites (this is where the COPPA trap comes into play).

Warning! – your online business is almost guaranteed to be shut down if you violate COPPA. The FTC very aggressively enforces COPPA.

The COPPA Trap Prior to July 1, 2013

The FTC case against Sony is probably the best illustration of what is known as the COPPA trap prior to the expanded rules effective on July 1, 2013.

On December 11, 2008, the FTC announced its agreement with Sony BMG Music Entertainment in which Sony agreed to pay $1 million to settle the FTC's COPPA claims. Specifically, the FTC's charges were based partially on information collected by Sony regarding the date of birth provided by registrants to Sony's social networking sites.

The key fact here is that Sony's sites were "general audience" sites -- that is, their sites are not "directed to children":

- Sites that are clearly “directed to children” fall easily within the regulation of COPPA.
• However, general audience sites also are regulated if they "knowingly collect personal information" from U13s, and that's where Sony fell short according to the FTC.

Sony represents hundreds of musicians and entertainers, some of which are popular with children and teenagers. To promote these artists, Sony operates over 1000 related websites. Many of these sites provide social networking opportunities including functionality providing for personal fan pages, reviews of albums, uploading comments, posting comments, and private messaging.

As part of the registration for many of Sony's sites, Sony required users to provide personal information, including their date of birth. Approximately 30,000 U13s provided their dates of birth which resulted in Sony having knowingly collected information from U13s, without first getting parental consent.

The FTC alleged additional COPPA violations including failure to provide sufficient notice of what information is collected from children, how it uses and discloses this information, and failing to provide parents with a reasonable means to review the information collected.

Tip – Review your registration pages to see if you have collected age-indicating personal information such as age, date of birth, or school grade; if so, remove these fields from your registration process, and for the information already collected from U13s, the best recommendation is to see an attorney for a possible remedy before it's too late.
Tip – Review your site to see if there is any page or pages that may inadvertently directed to children -- even if your site as a whole is not directed to children, if a single page is directed to children, you should modify it or comply with COPPA.

Tip – If you want to age-screen registrants, you should use a methodology that is age-neutral -- that is, a methodology that does not encourage children to lie about their age (for example, don't stipulate that "you must be 13 or over to register"), and if you ask for a date of birth, collect only the month and year, not the day.

The lesson to be learned from the Sony case is that general audience sites are not immune from regulation by COPPA. If you operate a general audience site, follow the 3 tips, but by all means, see an attorney - a COPPA violation is a very serious matter.

**COPPA Rules Prior to July 1, 2013**

If COPPA applies, regardless of whether your website is “directed to children” or if you "knowingly collect personal information” from U13s, there are certain specific rules that must be strictly followed.

The following is not a complete list of the COPPA rules, but it does provide a general understanding of what is involved in COPPA compliance:
clearly and prominently provide a link on your home page to your website’s information practices;

include in your Privacy Policy specific information about who is collecting the information, what is being collected, how it is being collected, and how it is being used;

before you begin collecting from a child, you must obtain verifiable consent from the child’s parent;

you must give the child’s parent the option to stop information from being shared with third parties;

you must provide a procedure for the parent to have the personal information deleted.

New COPPA Rules Effective on July 1, 2013

After an extensive investigation into the COPPA rules the FTC announced long-awaited amendments that are effective on July 1, 2013.

The new COPPA rules (summarized):

implement new COPPA compliance requirements for plug-ins and advertising networks;

add new categories of privacy-protected information, including persistent identifiers and physical location information;

supplement the definition of "directed to children" to add criteria and clarify when age-screens are appropriate;
Top 7 Gotcha’s That Can Shut Down Your Online Business

- clarify the required language for direct notices to parents;
- supplement the consent mechanisms available to operator;
- clarify safe-harbor processing requirements and add reporting requirements for safe harbor providers; and
- expand COPPA's security requirements to third parties that receive information from operators.

One of the key affects is the expansion of privacy-protected information regarding U13s. Under the new rules, the following are now regulated as privacy-protected information:

- screen names (where it functions as online contact information);
- photo, video and audio files that contain a child's image or voice;
- physical location data; and
- persistent identifiers that can be used to recognize a user over time and across different websites or online services, such as an IP address, or unique device identifier.

In addition, the “directed to children” rules have been expanded to include:
- the addition of musical content and the presence of child celebrities and celebrities that appeal to children to the list of criteria used to determine whether a website or online service is "directed to children";

- an actual knowledge standard for a plug-in, ad network or other property; and

- provisions outlining when an operator is permitted to age-screen to differentiate among users.

**Warning!** – Under the new, expanded COPPA rules, it is significantly easier and more likely for a general audience website to become regulated, thereby falling into the COPPA trap.

**Tip** – If you believe you’re regulated under the new, expanded COPPA rules, see an attorney immediately! Don’t try to go it alone!
Option 1: Hire an Internet Attorney

Your first option, and it’s the best option, is to hire an experienced Internet attorney. It’s always recommended that you hire an Internet attorney.

But there are also questions with this option:

- How to source, how to find an Internet attorney you can trust and have confidence in. The best source is to get a referral from someone you trust. The next best source is the martindale.com website. And be sure to look for the AV rating, it’s the highest rating they give.

- There’s also questions about turnaround time – sometimes working with a busy attorney doesn’t quite fit your tight schedule when you’re trying to get a new site online fast.
• However, the big question, and I talk to a lot of potential clients about this - is how much does it cost? I’m here to tell you that it can be expensive. I’ve had new clients tell me they were routinely quoted $3000 to $4,000 for legal fees to set up a new website.

• And what about keeping your site legally compliant? There would be additional fees from time to time to keep your site current with new legal developments.

So, bottom line, an Internet attorney is ALWAYS your best option, but is it within your budget? This isn’t a problem for the big guys on the web who rely heavily on their law firms, but it’s a real problem for the smaller entrepreneurs.

Option 2: Purchase Cheap, Downloadable, Cookie Cutter Forms. Do You Really Want To?

If you don’t have the budget to hire an Internet attorney, then you might be tempted to purchase some of those downloadable, cookie cutter forms from the Internet.

You know, the generic forms that are all basically the same – one size fits all.

But if you think about it you’ve probably got some lingering doubts about these forms:

• Does the generic form really fit my specific requirements of my site?

• Do you know how to use the forms?
Top 7 Gotcha’s That Can Shut Down Your Online Business

- Do you even know who created the darn things?
- What’s their background? I even know of a site where the attorney spokesperson doesn’t even practice Internet law, but he’s the spokesperson who sells these downloadable forms.
- And are these forms ever updated?
- Just to name a few.

So, do you have confidence that these downloadable forms are a real legal solution you can have confidence in?

Probably not.

Option 3: Internet Marketer Pro 2.0 Online Service

I’d like to tell you my story.

It all began back in the late ‘80s.

That’s when my software law practice was really humming, and I was working with a lot of clients who required relatively complex legal documents:

- Enterprise Software License Agreements,
- Software Distribution Agreements,
- Software Reseller Agreements,
- Private label Reseller Agreements,
- Software Publishing Agreements, and
- Software OEM Agreements.
I was using the cut and paste method.

And it was driving me crazy!

Why? The documents were too complex for cut and paste to be efficient.

I was always looking for the right form.

And even then, I was always worried about leaving something out of the transaction I was working on because the form I was using was based another transaction.

So, in the early 90’s, I bought a book on document automation. It was all about how to create a system that would automate the process of document creation.

It wasn’t about forms and templates.

It was about how to build in logic so that the system would be “intelligent”. A system that would enable me to create logic pathways, such as:

- Is the license non-exclusive? or
- Is it exclusive?

And depending on my selection of the option, it would provide additional relevant options, pathways, and decisions to make regarding the finished document.

The result would be a customized document – a document that once the system was programmed with all of my knowledge regarding an OEM agreement (for example), would include all of the relevant options and related clauses.
Bottom line, it would be a bear to program. But once programmed, it would almost be a magic tool.

But, I’m not a programmer, even though I had a Fortran IV course in grad school. I knew my limits.

So, I used the merge text functionality in a word processor. It enabled me to create question with a “yes” or “no” answer. And you could write a logic statement based on simple yes-no logic:

- “yes” would include the paragraph, and
- “no” would not include it.

I created a complex OEM agreement. It took a long time.

And it worked. But, there was a huge draw-back. The number of clauses was so large that the system was too unwieldy to be efficient to modify and to work with.

And later, a software client suggested that a database-centric approach would be a significant improvement. The clauses would be loaded in a database and external logic would determine whether to add the paragraph and where it would be located within the document.

Technically, it would be a system that incorporated methodology known as “rule-based document assembly”.

So, I designed the system, and he programmed it.

The result (after the difficult and time-consuming process of creating the logic and loading the database) was almost like magic!
It was like replacing an axe with a power saw.

It almost made document creation fun!

Much later, another client suggested that I make a product out of my rule-based document assembly system.

So, in 1996, we created a website – digicontracts.com – and added downloadable software and the database of legal documents designed for software companies.

Finally, in 2000, we ported the system to my website so that all the processing would occur on the server, and the finished document would be delivered by email.

It was one of the first systems incorporating what is known today as “software as a service” or “SaaS”.

For users, there was no software to download and install. The software remained on the server. All a user had to do was:

- simply login with an ID and password,
- select a document from the menu,
- answer a series of questions,
- then with the click of a Submit button, assemble a document on the fly for immediate download.

The output was a .txt file that could be copied into any word processor for further editing.

And most important, the output was:

- a customized document,
- with all the clauses numbered and formatted as they should be.
And we’re still using this software today on the digicontracts.com website.

Before the tsunami of new laws for websites began in 2009, I could see it coming. So, I created packages of documents designed for Internet marketers and online entrepreneurs for:

- website legal compliance,
- intellectual property protection
- direct marketing (to customers), and
- indirect marketing, such marketing via affiliates and resellers.

We called the package designed specifically for Internet Marketers and online entrepreneurs “Internet Marketer Pro”.

I named my rule-based document assembly “Digi Bot”. Rather than refer to it as “The Software”, it now had a name and personality, Digi Bot.

Think of Digi Bot as a very intelligent personal legal assistant that’s been programed to replicate me, to the extent you can with a software tool.

And this is the same software system I use every day in my Internet law practice. The is the magic tool that transformed my law practice.

I didn’t just cobble together some cheap forms for sale on the Internet.

Here’s the best example I can give of the power and intelligence of Internet Marketer Pro and that I designed onto the Digi Bot software.
Suppose you’re not sure which legal documents a specific website needs. It could be a combination of 15 or more legal documents, depending on what the site offers and related marketing practices.

This is where Internet Marketer Pro with Digi Bot comes to the rescue. You have the option to “Create All Documents For A Single Website In a Single Session”.

Digi Bot will ask you a series of questions. Your answers will indicate which documents are needed for your specific website. Digi Bot will remember the documents indicated. Then, automatically and seamlessly, Digi Bot will ask you the relevant questions for creating each of these documents.

And Digi Bot is even smart enough not to ask the same question twice!

At the conclusion of the questions, Digi Bot will assemble, generate, and deliver the customized documents in a few seconds.

Later, in 2012, I realized that something very important was missing.

It became clear to me that it wasn’t just about documents. It was also about understanding what I call the “Rules of the Road”.

Documents alone without:

• understanding how to use them, and
• how to operate an online business legally,

was just half a legal solution!
So, I created tutorials in the form of:

- easy 5-minute videos,
- user friendly special reports, and
- quick-start cheat sheets.

I boiled the rules down to their essence so they would be quick and easy to understand and follow.

We integrated the tutorials into the document packages, and we renamed it: “Internet Marketer Pro 2.0”.

And we believe Internet Marketer Pro 2.0 accomplishes my Mission Statement:

- To *empower* you with a Simple Online Legal Solution…
- so you can be as successful as you want, and to grow your online businesses, as fast as you want…
- with the *confidence* that you’re as legally protected as the Big Guys who can afford to hire expensive law firms,
- but without the high cost!
Tip: A complete online legal solution, absolutely, positively must include both:

- intelligent software to create customized legal documents, and
- easy-to-understand tutorials for the Rules of the Road.

If it doesn’t, then it’s not a complete solution!
Conclusion

Is There Any Doubt That The “Wild, Wild West” Days Are Over?

There should be no doubt that The "Wild, Wild West" days of the Internet are over.

The landscape has changed. We’re now in a new era.

Now, online commerce is highly regulated. Sort of like traditional, brick and mortar business.

But it’s not all bad.

Think of it this way: All Internet marketers and online entrepreneurs are also consumers. And most of the regulation protects consumers from being ripped off by scammers.

The thing is… Internet marketers and online entrepreneurs need to develop a new mindset – one that embraces the new era in a more positive way.

A mindset that recognizes that legal compliance creates consumer confidence. It builds credibility. You know, that old marketing cliché: know, like, and trust.
Consumers are becoming more Internet savvy. And this includes concerns relating to online privacy and good old fashioned best business practices.

When I shop online, I always check out the website Privacy Policy. I don’t read all of it, but I usually check to see sharing policies. Above all, I check to see if it appears up-to-date.

An online business’s Privacy Policy is a good barometer of how they operate their business. Are they informed about regulations in the new era? How they treat their Privacy Policy is an excellent indication.

So, if I see what looks like an out-of-date, boilerplate Privacy Policy, my level of confidence is affected – negatively! The website is not credible, in my opinion, and I usually take my business elsewhere.

And more and more consumers are beginning to think this way. Believe me.

**The Legal Gotcha’s**

There are a lot of legal Gotchas. I’ve chosen what I believe are the Top 7 Legal Gotchas. The ones you absolutely, positively need to avoid. Right now.

Additional Gotchas are presented in the Appendixes. They’re important, but they didn’t make the cut for my Top 7 list.

The Gotchas presented in this book are not presented to frighten. Instead, they should be perceived as issues that responsible online marketers should deal with.
For protection of your online business, yes.

For the protection of your personal assets, definitely yes!

But also, for a statement reflecting the best practices that you follow in your online business.

Don’t fall into the trap of thinking that these Gotchas only affect the Big Guys. They apply to all online businesses - to Internet veterans and to new travelers on the road to online success.

And they have one thing in common – all of them can be avoided!

And remember this: if you don’t take action to avoid the Gotchas, then you’ve made a conscious decision to put yourself, your personal assets, and your family, at risk.

All you need is the commitment to do it the right way. Plus, the necessary documents and information to guide you.

And if you do it the right way, your journey along the road to online success will be a much safer and more rewarding one. Trust me on that!
Appendixes

Legal Gotcha’s That Didn’t Make The Top 7 List
Appendix 1

FTC Accelerates Crackdown
On Fake News Sites

We’ve all seen headlines in search results like this one – “XYZ Exposed: Miracle Diet or Scam”. And perhaps we actually believed there was objective reporting or unbiased commentary behind the headline. But after reading the web page, it was clear that the headline was just a clever way to catch your attention and lure you to a sales page with an aggressive sales pitch.

The Federal Trade Commission (FTC) has seen these headlines too, and the FTC doesn’t think they’re clever at all. In fact, the FTC believes they constitute deceptive and unfair trade practices, as indicated by the FTC’s accelerated crackdown on affiliates of a popular diet drink with aggressive weight loss claims.

Modus Operandi

The modus operandi of these sites was to start with attention grabbing headlines such as the one listed above and these additional ones - “News 6 News Alerts,” “Health News Health Alerts,” or “Health 5 Beat Health News.”

The sites presented what appeared to be a skeptical commentator who raises the question of whether the diet
drink is really effective. The commentator appeared to be objective; however, after a few paragraphs the commentator would conclude that use of the diet drink would result in a 25-pound weight loss in 4 weeks - all this without changing diet or exercise according to the FTC. The prices for the supplement ranged between $70 and $100.

The FTC’s Claims

When the FTC originally initiated law suits against these sites, Charles Harwood, Deputy Director of the FTC’s Bureau of Consumer Protection stated: “We are alleging that nearly everything about these Web sites is false and deceptive”. In addition, the FTC pointed out that the defendants aggressively promoted the deceptive ads by spending millions of dollars for placement on high volume websites resulting in millions of views by consumers and substantial sales.

Specifically, the FTC contended that the offending sites:

- failed to disclose their material relationships involving the payment of affiliate commissions with the merchants of the products;

- failed to produce independent tests to support the claims made prior to public dissemination;

- included a section of “consumer comments” that were completely fabricated;

- used infringing logos of reputable media outlets such as ABC, Fox News, CNN and Consumer Reports to give the false impression of credibility; and
• misappropriated the image of a French reporter for use on the sites.

**The Settlements**

The cases brought by the FTC were against six affiliates of the merchant that manufactured and supplied the weight loss supplement.

In the settlements, the defendants agreed that they will permanently cease their allegedly deceptive practice of using fake news websites. In addition, the settlements require that the defendants cease making deceptive claims about their other products, including work-at-home schemes and penny auctions which most of them promoted.

The big hammer in the settlements included fines in an aggregate amount which represented the affiliate commissions the defendants received through their fake news sites.

These settlement results clearly indicate that the FTC aggressively pursued every dollar they could under the circumstances (the final amounts left most of them with few real assets, if any):

• one defendant’s $2.5 million judgment was suspended when he pays $280,000 and records a $39,500 lien on his home;

• another defendant’s fine of $204,000 was suspended pending the payment of $13,000 plus the proceeds from the sale of a BMW automobile, and
still another defendant was suspended pending the payment of almost $80,000 over a 3 year period.

Conclusion

The take-aways from these cases include:

- fake news sites are virtually guaranteed to get you sued by the FTC,
- ditto for fake testimonials or user comments,
- diet supplements of any kind are high on the FTC’s radar screen for regulatory scrutiny,
- the FTC is serious about enforcing its guidelines that affiliates are required to conspicuously disclose the fact that they are paid commissions for endorsements,
- consistent with the FTC’s long-standing policy, advertising claims should be substantiated prior to public dissemination.

The FTC continues to make it absolutely clear that the days of the “Wild, Wild West” on the Internet, when it was open season on deceptive marketing practices, is clearly over for good.
Appendix 2

Deceptive Website Legal Forms Result in $359 million FTC Settlement

In a recent settlement, the Federal Trade Commission (FTC) made it clear that deceptive website legal forms, particularly those that support “free” offers, will not be tolerated.

According to the FTC, the deceptive marketing schemes employed by the defendants netted over $450 million in sales. The result - the FTC came down hard on the defendants, with one individual defendant giving up all the money in his bank accounts, his house, automobile, and other personal property.

The takeaways from this settlement provide clear guidelines for all Internet marketers, particularly those who with sites that use “Free” offers as a lure for upsells to provide recurring revenue, or so-called “continuity” websites.

The Marketing Schemes

The offers were for products with broad market appeal, including weight-loss pills, teeth whiteners, health supplements, work-at-home options, access to government grants, free credit reports, and penny auctions.
A key factor in the marketing scheme was the lure of “free” offers, including “free” trials. Consumers were often charged a monthly fee, typically $79.95, plus additional monthly recurring fees for “bonus” offers and upsells.

Another key factor in the marketing scheme was significant leverage through affiliates – who drove traffic to the websites with the offers through widespread use of banner ads, pay-per-click ads, pop-ups, and unsolicited email. Affiliates were paid commissions for the sales resulting from traffic sent to the offering websites.

The Devil Is In The Details

Neither of the above key factors in the marketing scheme are per se illegal. The problem, according to the FTC, is in the details of how the defendants used the key factors to deceive consumers in violation of the FTC Act.

The following checklist summarizes the deceptive elements alleged by the FTC.

• Misrepresentations About “Free”, “Risk-Free”, and “Bonus”. The primary lures for consumers were the “Free” offers. The defendants induced consumers to provide their credit or debit card information by falsely promising that the product or service could be acquired on a “free” or “risk-free” trial basis while only paying a nominal shipping and handling fee. Some offers represented that the consumer would receive a product or service as a “bonus” for simply signing up. In fact, consumers were charged for products or services that they didn’t know about or had not agreed to purchase, and in some cases the charges were recurring on a
monthly basis. The process for cancelling these charges or obtaining refunds involved separate time-consuming phone calls and other steps designed to significantly increase difficulty.

- **Failure to Disclose, or Deceptive Disclosure of, Additional Charges.** Despite the “free” offers, there were additional charges. In some cases there was no disclosure of additional charges. In many cases, there were disclosures regarding the additional charges, but the disclosures were not in a clear and understandable manner. Additional terms were buried in a separate “terms and conditions” page loaded with “lengthy, legalistic fine print” that was not accessible from the ordering page. Consumers were not required to click on an “I Agree” button to indicate acceptance with the “terms and conditions” page.

- **Deceptive Refund Policies.** Another significant lure for consumers were generous refund offers. Promises included “100% Satisfaction Guarantee”, “Risk Free Guarantee”, and “Easy Money Back Guarantee… Just Follow the 3 Easy Steps”. In fact, refund requests were denied, or if promised, they were never issued. In many cases consumers had to resort to complaints to law enforcement or the Better Business Bureau to actually get a refund.

- **Failure to Disclose, or Deceptive Disclosure of, Limitations on Cancellations and Refunds.** Despite the refund offers, there were limitations on cancellations and refunds which were either not disclosed or not adequately disclosed.
• False and Unsubstantiated Efficacy Claims. The defendants did not possess or rely upon a reasonable basis to substantiate their advertising claims on banner ads approved by the defendants for use by affiliate marketers.

• False Celebrity and Other Endorsements. The defendants displayed images of celebrities on their websites without permission and falsely represented that these celebrities endorsed the defendants’ products. In addition, logos for prominent news entities were displayed with statements such as “Featured On” and “As Seen On TV”, when in fact none of these entities endorsed or positively reported on any of the products.

• Evading Risk Management Rules to Obtain Merchant Accounts. The defendants submitted inaccurate financial information to merchant banks in order to retain or obtain merchant credit card processing accounts.

The Settlement

The settlement included substantial payments by the defendants from the sale of business and personal assets. In addition, the defendants’ were enjoined for future violations of the deceptive practices discussed above.

Finally, regarding their affiliates, the defendants were ordered:

• to disclose to all affiliates that engaging in deceptive practices would result in immediate termination, and
to monitor affiliate activities monthly for violations.

Conclusion – Important Settlement Takeaways

Most of the takeaways from this settlement are obvious egregious violations. However, there are three takeaways that are perhaps no so obvious, but which are significant for Internet marketers:

- reliance on disclosures or disclaimers in website legal documents alone is not enough to avoid liability; in this case there were disclosures regarding additional charges and refunds limitations, but they were buried in the “fine print”, and therefore, they were not clearly and conspicuously disclosed in order to avoid consumer deception;

- even if disclosures are clearly and conspicuously disclosed, using “Free” offers as a lure for upsells, particularly if the upsells involve recurring revenue (continuity plans), will always be a red flag issue, and therefore, attract close scrutiny by the FTC; and

- using affiliates to advertise and drive traffic for sales does not absolve an Internet marketer merchant from liability for the affiliates’ deceptive practices; monitoring of affiliate marketing practices and termination of offending affiliates is required.
Top 7 Gotcha’s That Can Shut Down Your Online Business
Appendix 3

FTC Liability Traps Internet Marketers Must Avoid With Affiliate Marketers

Internet marketers often ask: Am I liable if any of my affiliates engage in deceptive marketing practices? The answer is, it depends. This article will provide a checklist of practical points that will help Internet marketers determine what is required for their specific affiliate marketing program and FTC legal forms.

We only have to look to recent FTC cases to learn that affiliate marketers have been nailed for engaging in deceptive marketing practices involving false and unsubstantiated claims, false news reports, untrue claims of test results, and testimonials that were completely fabricated. And in one recent case, an Internet marketer with ineffective FTC legal forms has held liable for failing to monitor affiliates’ marketing practices.

Internet marketers should understand that the legal violations of affiliates may result in liability for the Internet marketer, particularly where an Internet marketer fails to monitor and terminate affiliates who engage in deceptive marketing practices. For this reason, it’s absolutely critical that Internet marketers who use affiliates understand how to avoid this liability.
Basic Truth In Advertising Principles

To begin to understand how an Internet marketer may be held liable for affiliates’ deceptive marketing practices, it’s important to understand four basic truth in advertising principles that apply generally to all marketers, including both Internet marketers and affiliates.

- Claims by marketer regarding a product or service that would materially influence a consumer’s decision must be truthful, not misleading, and reasonably substantiated prior to publication. Being truthful is a no-brainer. However, if the claim is technically true, but it omits a material factor that a consumer would consider, then it would also be deceptive. And claims about objective, specific results must be substantiated by tests prior to publication or else they’re also deceptive.

- Ditto for claims made endorsers and testimonialists about someone else’s product or service. The same rules summarized above also apply to endorsers and testimonialists who make claims or statements about the products of others.

- If a marketer doesn’t have proof that an endorser’s “success story” experience represents what consumers will achieve by using the product, the advertising copy must clearly and conspicuously disclose the generally expected results in the depicted circumstances. Prior to December, 2009, it was OK to use an endorser’s “success story” endorsement, even if the endorser’s level of success was significantly greater than typical, provided that a “results not typical” disclaimer
accompanied the endorsement. Beginning in December, 2009, the “results not typical” disclaimer will no longer be effective. Now, a statement regarding the generally expected results is required.

- If there’s a “material relationship” (family or employment relationship or payment or benefits) between the marketer and an endorser or testimonialist that would affect how people evaluate the endorsement or testimonial, it should be disclosed “clearly and conspicuously”.

**The Problem With Affiliate Marketers**

Affiliate marketers are engaged in performance marketing, meaning that they are compensated on a “performance” basis involving a completed action. In most situations, affiliates are compensated based on conversions originated through traffic driven to the advertiser’s website.

The problem with affiliates in terms of marketing practices is that their performance-based compensation creates an inverse relationship between maximizing conversions on the one hand, and on the other hand, providing marketing messages that comply with the truth in advertising rules discussed above.

**What is Required If You Market Through Affiliate Networks**

The FTC requires that Internet marketers have reasonable programs in place to train and monitor their affiliates.

The key question is what is “reasonable” according to the FTC? The FTC says that what is reasonable varies with the
circumstances. According to the FTC, if the product or service at issue could cause consumer harm – either physical injury or financial loss – then a relatively high level of supervision would be required. For example, health products may require more supervision than the promotion of ladies hand bags.

Core elements of an affiliate monitoring program should always include:

- Consistent with a marketer’s responsibility for substantiating objective product claims, Internet marketers should explain to affiliates the marketing message regarding the product or service, including what can be said and what can’t be said about the product or service. These explanations should be consistent with the basic truth in advertising principles discussed above.

- Set up and maintain a reasonable monitoring program to determine what affiliates are actually saying about the product or service.

- Follow up with questionable affiliate marketing practices, and terminate affiliates who willfully or repeatedly do not follow the rules.

A recent settlement with an Internet marketer imposed more stringent requirements.

- Clearly and conspicuously disclose in writing to each marketing affiliate that engaging in deceptive marketing practices will result in immediate termination of the affiliate relationship and forfeiture of all monies owed to such marketing affiliate.
• Routinely monitor and review, on at least a monthly basis at times not disclosed in advance to the affiliate and in a manner reasonably calculated not to disclose the monitoring activity at the time it is conducted, affiliate marketing materials, including websites, emails, banners, sponsored search terms, and pop-up ads.

• Promptly and completely investigate any consumer complaint regarding any affiliate.

• Immediately halt the processing of any payments or charges generated by an affiliate that the Internet marketer knows or should know is engaged in a deceptive marketing practice.

• Fully refund, within five business days, each consumer charged by any defendant whose sale originated from any affiliate engaging in a deceptive marketing practice.

• Terminate immediately any affiliate that is engaged in deceptive marketing practices.

Conclusion

Internet marketers who do not monitor and manage their marketing affiliates regarding deceptive marketing practices do so at their peril. Both the FTC and state regulatory authorities are becoming increasingly more vigilant regarding online advertising and marketing, particularly regarding affiliate marketers.
At the very least, Internet marketers should implement programs consistent with the core elements discussed above. It remains to be seen whether the more stringent requirements implemented in the recent FTC settlement with an Internet marketer who was actively engaged in deceptive marketing practices himself will also apply to Internet marketers who have no past record of deceptive practices.
Appendix 4

Why It’s Risky To Copy Stuff Off The Web

It’s tempting and so easy to use your right click to download stuff off the Web – to copy or save images, text, even videos. And this content is often great material for your website copy, squeeze page, sales page or banner ad.

Fair warning – in most cases this content will be protected by copyright even if there is no copyright notice, and you will need a license or a valid claim of fair use to use it, or face a possible copyright infringement claim that could result in liability of up to $150,000 in damages.

The Rule of Automatic Copyright

The key to understanding why most content on the Web is copyright protected, even if it doesn’t have a copyright notice, is sometimes referred to as “The Rule of Automatic Copyright”.

How copyrights are created is really simple, and that’s why it’s so often misunderstood. The Copyright Act says that a work is created when it is “fixed in a tangible medium of expression”. This means that a copyrightable work of authorship is created when pen hits paper, or keystrokes are recorded into the RAM of a computer, or video is recorded.
So, the fundamental rule is that copyrights are created automatically when an original work of authorship is fixed; no registration, copyright notice, or other act is required. And the copyrights vest in the author of the work. The copyright owner then controls to what extent another person can exercise the exclusive rights of a copyright owner – the rights to copy, modify (create derivative works), distribute, display, and perform the work.

And very important, if you exercise of any of these exclusive rights without permission (a license) or a valid claim of fair use, you’re a copyright infringer subjecting you to claims for damages, in addition to other remedies.

What Is Fair Use?

Fair use is a basic principle of copyright law that says that the general public may use certain portions of a copyrighted work without a license from the copyright owner, provided the use is for purposes such as commentary, criticism, search engines, news reporting, research, teaching, library archiving or scholarship.

The catch is that if the copyright owner disagrees with the validity of your fair use claim, you may have a copyright infringement lawsuit on your hands.

To determine whether you have valid claim of fair use, four factors must be considered:

- the purpose and character of the use, including whether the use is a commercial use or for non-profit educational purposes, including the “transformative” nature of the use;
• the nature of copyrighted work;

• the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

• the effect of the use upon the potential market for or value of the copyrighted work.

The process of weighing and applying the four factors is fact intensive, and there is no bright line test. For example, with the first factor, a key question that weighs in favor of fair use is whether you have transformed the portion of the original work by adding new expression or meaning, such as with a parody, or by adding independently created images to quotes taken from a copyrighted article or speech.

Probably the most significant of the four factors in the context of use in connection with promotional material for your website copy, squeeze page, sales page or banner ad is the fourth factor – the effect on the potential market for the copyrighted work.

One final tip – don’t fall into the trap of believing that if you acknowledge the copyright owner of the source material, your use is a fair use. On the one hand, acknowledgement may be a point to consider in weighing the four factors, but in and of itself it won’t protect against an infringement claim. And what’s even worse, it may even create additional legal claims involving infringement of privacy rights.
Conclusion

Bottom line, it’s very risky to freely use your right click to download stuff off the Web. Copyrights to Images, text, and videos are almost always vested in someone. And the fair use defense to copyright infringement is very limited in scope, and generally poorly adapted for use with your website copy, squeeze page, sales page or banner ad.

It’s always best to get a license. That’s the only way to be sure that you’ll not be facing a copyright infringement claim and a possible claim of up to $150,000 per work.
Appendix 5

The FTC Begins Crackdown On Behavioral Ads - Is Your Site In The Cross Hairs?

On March 14, 2011, the Federal Trade Commission (FTC) announced its first behavioral advertising settlement. If your website collects behavioral data or serves behavioral ads – either directly or indirectly through the use of behavioral ad vendors – you need to understand and comply with the FTC’s notice and choice principles, or suffer the consequences.

What Is Behavioral Advertising?

Behavioral ads are based on anonymous data collected on how a user’s computer browses the Internet, including websites visited, searches made, and content read. This data is used to create a behavioral profile that is linked to a specific demographic. The ads seen by the computer’s user are tailored to the user’s interests resulting in significantly increased relevancy and sales.

Contextual ads, in contrast to behavioral ads, are based solely on the content of the specific website page the user is viewing. Because contextual ads are generally not as relevant to the user’s interests as behavioral ads, contextual ads are less effective, and therefore less profitable.
Although behavioral data is essentially anonymous when collected, the FTC and privacy advocates are concerned that the amount and depth of some data could lead to personal identification of users. In addition, even if users are not personally identified, the enhanced data about them could rise to the level of an invasion of privacy.

The Chitka Settlement

In 2009, the FTC issued a staff report on behavioral advertising that explained the FTC’s principles regarding behavioral data. The FTC believes that its deceptive and a violation of the FTC Act to fail to provide to consumers proper notice and opt-out choice regarding the collection of behavioral data. The FTC’s settlement with Chitka, Inc. is the first settlement based on these principles.

Chitka is an intermediary between advertisers and websites that serve ads for the advertisers. To collect behavioral data, Chitka passes a cookie on users’ computers and then uses the cookie to tracks the users’ online behavior.

The FTC alleged in its Complaint that for over two years Chitka advised consumers that if they wanted to opt out of behavioral tracking they could click on a button titled “opt out”. Clicking the button would generate a message that read “you are opted out”. The catch according to the FTC is that the opt out lasted only for ten days, and then new cookies would be passed to consumers’ computers resulting in tracking of behavioral data for serving behavioral ads.

In its settlement with the FTC, Chitka agreed to:

- delete all identifiable user information collected ineffective opt out period,
• provide consumers with a new opt out mechanism that lasts for at least five years, and

• notify consumers whose opt out was ineffective to opt out again.

Chitka also agreed to a notice and opt out procedure that could be interpreted as a blueprint for what the FTC believes is generally required for all sites that collect behavioral data. This procedure includes:

• A message on the home page that reads “we collect information about your activities on certain websites to send you targeted advertisements. To opt out of [our] targeted ads, click here.”

• The “here” link points to an opt out page where the user is notified that opt out means the information would not be used for behavioral ads, the status of the opt out (in or out), and that opt out is limited to a specific browser and should be repeated if another browser is used.

• A link on any behavioral ad that reads “Opt Out?”, and that provides text when the users’ cursor hovers over the ad that reads “Opt Out of Targeted Ads”. The Opt Out? link would point to the opt out page described above.

Conclusion

The Chitka settlement clearly establishes that the FTC believes it’s a deceptive practice under the FTC Act to fail to provide notice and opt out choice regarding behavioral
ads. What’s more important is that the notice and opt out procedure agreed to in the settlement may be a clear indication of the specific procedure that the FTC requires for compliance.
Appendix 6

FTC's Settlement With Google Provides Game Changing Internet Privacy Regulations

You’ve certainly heard about Google’s highly promoted BUZZ service which is designed to compete directly with Twitter by offering much of Twitter’s basic functionality with a Facebook-like platform including location data integrated into Gmail. What you may not have heard is that the Federal Trade Commission (FTC) recently made BUZZ the poster child for the FTC’s effort to show that the old tried and true privacy protection methodology is now not enough.

Once again, the FTC has upped the ante for privacy requirements, and all websites are expected to comply with the new game changing regulations, or face the consequences.

The FTC’s Allegations

On March 30, 2011, the FTC announced a proposed consent order regarding Google’s BUZZ service. According the FTC, Google had engaged in deceptive practices regarding discrepancies between its privacy policy statements and its actual practices regarding BUZZ.
Google’s privacy policy stated in part: “When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use."

When Google launched BUZZ, Google invited its Gmail users to sign-up with two options:

- “Sweet! Check out Buzz”, or
- “Nah, go to my inbox”.

The FTC alleged that both of these options were deceptive. The “Sweet” option was allegedly deceptive because users were not clearly informed that the identities of certain of their email recipients would be made public by default. The FTC claimed this was contrary to Google’s promise to obtain consent for new information uses and also in violation of Google’s requirements in its self-certified participation in the US-EU Safe Harbor program.

The “Nah” option was allegedly deceptive because users were unwittingly enrolled in certain parts of BUZZ despite selecting “Nah”.

The Game Changers

As part of the proposed settlement, Google is required to implement a comprehensive privacy program with very specific mandated requirements and to undergo privacy audits over the next twenty years. This requirement is not new. The FTC has historically signaled its expectations through consent orders with similar requirements.
What’s new, and certainly game changing, are the following.

- Covered Information. Up to now, privacy regulations has focused on “personal information” that may be used to identify an individual person. From now on, the focus will be on “covered information” which the FTC construes to cover additional elements including screen names, location data, and lists of contacts.

- Privacy by Design. Generally, privacy by design is a holistic approach where privacy compliance is designed physically into systems from their inception, rather than waiting to address compliance the end of the design process or separately through a published privacy policy. Although at this time there is scant information regarding privacy design specifics, a safe bet is that privacy by design will involve pop-up or interstitial messaging regarding the use and sharing of covered information at the time a user discloses information or opts in to a specific program. This is in stark contrast to the current practice of providing all such messaging in a separately published privacy policy.

**Conclusion**

With the proposed BUZZ settlement, the FTC has aggressively raised the bar in terms of privacy requirements for all online businesses. In essence, the FTC settlements have created “common law” regarding privacy, and websites that fail to comply do so at their peril.

Expect more specific information regarding the game changers in the form of additional suits and settlements by the FTC in the near future.

117
Top 7 Gotcha’s That Can Shut Down Your Online Business
Appendix 7

Internet Marketers – Are You Liable For Your Affiliates’ Trademark Infringement With Sponsored Keyword Ads?

You’re an online retailer, and you’ve got a network of affiliates that are committed to selling your products. You expect that your affiliates will engage in online advertising to generate sales. Some of your affiliates will purchase keywords for sponsored ads from major search engines including Google and Bing, and some of these keywords may be trademarks of your competitors.

The purchase of a competitor’s trademark as a keyword is likely to result in litigation. Do your affiliates’ purchases of a competitor’s trademark for sponsored ads amount to trademark infringement? And if so, will you be held liable for your affiliates’ trademark infringement?

Keyword Ad Litigation Trends

The practice of selling and purchasing keyword ads that contain competitors’ trademarks continues to be hotly litigated. To date, most of the lawsuits filed by trademark owners have been aimed at the sellers of the keyword ads – the major search engines, primarily Google.
The current trend of the law seems to be that neither the sale of keyword ads using trademarks (by search engines) nor the purchase of these keyword ads (by advertisers) is inherently infringing by itself. The focus now seems to be shifting from the sale and purchase of the keyword ads to the precise wording of the ads generated by the keywords.

To date, there has been little if any guidance from court decisions regarding whether online retailers can be legally liable for keyword ad buys by their affiliates – that is, until the recent case of 1-800 Contacts v. Lens.com decided by a Utah U.S. District Court.

**1-800 Contacts v. Lens.com**

1-800 Contacts sued Lens.com for trademark infringement based on purchases by Lens.com and its affiliates of sponsored ads that contained 1-800 Contacts trademarks and variations of them.

The Court ruled that Lens.com was not liable for trademark infringement for its purchase of the keyword ads stating “… that the mere purchase of a trademark as a keyword cannot alone result in consumer confusion”. Also, the court noted that Lens.com had not used 1-800 Contacts exact trademark, only variations of it.

After dismissing 1-800 Contacts’ claim against Lens.com for Lens.com’s purchases of keyword ads and the wording of the ads the keywords generated, the court turned its attention to the issue of whether Lens.com was liable for its affiliates’ purchases of keywords ads. In its analysis of this issue, the court addressed:
• whether the keyword ads purchased by affiliates were infringing, and

• if so, whether the infringement by affiliates could be used to nail Lens.com.

Regarding the first question, the court focused on “… not just what keyword was purchased, but what was the language of the advertisement generated by that keyword”. The court ruled that some of the affiliates went too far in their ad copy because they used the exact 1-800 Contacts trademark. This caused a “strong likelihood of confusion” and therefore infringement.

Regarding the second question, the court ruled that the actions of Lens.com’s affiliates could not be imputed to Lens.com because Lens.com used the Commission Junction affiliate network to acquire its affiliates, and for this reason Lens.com didn’t know who most of the affiliates were and had little direct contact with them. The court noted that Lens.com had nothing more than “general information” of its affiliates and their activities, and ruled that [Lens.com] therefore cannot be charged with contributory infringement because Lens.com had no actual knowledge or willful blindness based on that information.

Conclusion

The 1-800-Contacts v. Lens.com case is important for keyword ad cases for at least two reasons:

• the court made it clear that it’s about the ad copy, not the ad buy, and
• online retailers won’t be automatically be held liable for infringing ads placed by their affiliates; the result will depend largely on what information the retailer had regarding the identities of the infringing affiliates and their activities, and what it did (or didn’t do) with that information.

Although this case is not the last word on the issue of a retailer’s liability for keyword ads placed by their affiliates, it does provide some guidance regarding where this emerging trend will lead us in the future.
Top 7 Gotcha’s That Can Shut Down Your Online Business

Appendix 8

3 CAN-SPAM Gotcha’s That Every Internet Marketer Should Avoid

Experienced Internet marketers often operate under the misconception that the CAN-SPAM Act doesn’t apply to most routine business communications. With CAN-SPAM Act fines of up to $16,000 per violation, this misconception could add up to a big number.

That’s why Internet marketers should avoid 3 gotcha’s that are CAN-SPAM traps for the unwary.

The CAN-SPAM Act

The CAN-SPAM Act of 2003 (CAN-SPAM) promised to provide remedies against annoying and unsolicited bulk email known as “spam”. Typical of legislation that starts out with limited objectives, CAN SPAM reaches much further than regulating unsolicited, bulk email – and that’s where the gotcha’s come into play.

Before we get to the gotcha’s, let’s review CAN-SPAM’s 5 basic rules as supplemented by amendments enacted in 2008:

- header information (identifiers such as To, From, IP Address): must not be materially false or materially misleading;
subject line: must not mislead the recipient about a material fact regarding the email’s contents or subject matter;

return email address: must contain a functioning email address that the recipient can use to request no further messages;

requests to unsubscribe: if a recipient requests unsubscribe from receiving additional emails, emails matching the unsubscribe request must be honored within 10 days with a mechanism that is available from a single web page and that operates with a single click; and

contents: the email must (i) clearly and conspicuously identify that it is an ad, (ii) provide clear and conspicuous notice the recipient may unsubscribe for additional emails, and (iii) contain a valid postal address for the sender (may include a valid post office or private mailbox address).

In addition to supplementing the 5 basic rules, CAN-SPAM’s 2008 amendments added an additional rule regarding email newsletters and other emails that have multiple advertisers, contributors, or senders. Under the new “designated sender” rule, multiple contributors to the email may designate as single sender who must be designated in the From line, and who will be responsible for CAN-SPAM compliance.

“Commercial” emails are required to comply with all 5 of the basic rules, plus the “designated sender” rule.
“Transactional or relationship message” emails are required to comply only with the header information requirement and the “designated sender” rule.

**Gotcha 1 – CAN-SPAM Applies Only to Bulk Email, Right?**

Not true.

Although much of the publicity surrounding the passage of CAN-SPAM focused on regulation of unsolicited, bulk email, there is no minimum number of emails for CAN-SPAM to apply; CAN-SPAM applies to even a single email.

So, if a single email relates to the business of an individual or entity, it’s a “commercial” email and CAN-SPAM applies, and the email is subject to all 5 of the basic rules, plus the “designated sender” rule.

**Gotcha 2 – CAN-SPAM Only Applies to Unsolicited Email, Right?**

Not true.

The Federal Trade Commission (FTC) made it clear that CAN-SPAM may apply to emails that are solicited. The FTC stated in regulations issued in 2008 that the FTC would view email newsletters that were subscribed to (or solicited by) a person to fall within the definition of a “transactional or relationship message” if the newsletter consists exclusively of informational content or combines informational and commercial content.
So, even if the email newsletter is solicited by the recipient, CAN-SPAM applies; however, as discussed above, as a “transactional” email, the sender is required to comply only with the header information requirement and the “designated sender” rule.

Gotcha 3 – Regular “Business-to Business” Emails are Not Covered by CAN-SPAM, Right?

Not true.

The FTC made it clear in 2008 that emails sent in connection with what most businesses view as “business-to-business” relationship emails may also be regulated as “commercial” emails under CAN-SPAM. For example, the FTC noted that “business-to-business relationship” emails could include mortgage lenders sending emails to brokers with the latest interest rate information or equipment leasing businesses sending emails to equipment vendors regarding rate sheets.

The FTC expressly rejected a request by business leaders to add a “business-to-business relationship message” category to the “transactional or relationship message” category discussed above. This means that “business-to-business relationship” emails are subject to all 5 of the basic rules, plus the “designated sender” rule.

So, even though this determination by the FTC regarding “business-to-business relationship” emails flies in the face of reason and common business practices, it’s the law according to the FTC.
Conclusion

With CAN-SPAM, as with many statutes, there are unintended consequences that sometimes lead to surprising results. Nevertheless, strict compliance with the rules involving the 3 gotcha’s is required in order to avoid liability under CAN-SPAM.
Appendix 9

If You’re Tempted To Use Fake Endorsements – Don’t Do It!

The Federal Trade Commission’s recent settlement with Reverb Communications is the FTC’s first case targeting deceptive advertising on the Internet since the FTC Guides were announced late in 2009.

If you use online endorsements or testimonials from others, you should review your internal marketing policies and your FTC website forms to avoid substantial liability for deceptive advertising.

The Reverb Communications Case

Reverb Communications is a public relations firm representing major clients in the video game industry, including clients such as MTV Games and Harmonix, as well as smaller firms that sell mobile game apps via the iTunes store. According to the FTC, Reverb’s fee often includes a percentage of the sale of its clients’ gaming apps.

The iTunes store provides users the ability to post reviews of gaming applications that are available for purchase. These reviews include a rating system (based on a possible rating of one to five stars) and written text.
According to the FTC, during a period of approximately one year Reverb employees posted reviews in the iTunes store favorable to games of Reverb’s clients. The reviews were posted in a manner that would convey the impression that disinterested consumers had posted them.

In addition to giving five-star ratings to Reverb’s clients’ games, Reverb’s employees posted written endorsements such as:

- “Amazing new game”,
- “ONE of the BEST”, and
- “Really cool game”.

The FTC brought suit claiming that Reverb engaged in deceptive advertising by having its employees pose as ordinary consumers posting reviews, while failing to disclose that the reviews were from paid employees working on behalf of their clients. Reverb agreed to settle the case.

**Lessons Learned**

The basic lesson is clear – don’t use employees or contractors to post fake endorsements under any circumstances.

The FTC stated in its press release announcing the Reverb settlement: “Companies, including public relations firms involved in online marketing need to abide by long-held principles of truth in advertising. Advertisers should not pass themselves off as ordinary consumers touting a product…”.
What if you post actual endorsements (not fake ones) from satisfied customers on your website – or if you allow bloggers to post endorsements on your site? What is required to avoid a deceptive advertising claim by the FTC?

If some of your endorsers receive a fee or some kind of benefit in connection with their endorsements, you need to place a link in close proximity to the endorsement that links to disclosure text such as:

- Some or all of the endorsers who provide testimonials or comments on this site regarding this site, its products or services may receive payment in the form of affiliate commissions, referral fees, or promotional materials or benefits from us.

- Although you might assume that these endorsements are biased by reason of compensation, to the best of our knowledge we believe these endorsements represent the honest opinions of the endorsers.

**Conclusion**

The FTC settlement with Reverb requires Reverb to remove the previously posted deceptive endorsements and to refrain from using employees to post fake reviews for its clients in the future.

The Reverb case indicates that the FTC is very serious about enforcement of its Guides that were announced late last year.

Expect more FTC enforcement actions in the near future.
Appendix 10

Website Advertising: 2 Legal Traps To Avoid When Writing Your Own Copy

If you're like most small ecommerce businesses, you're likely to write your own marketing copy. Be aware that this is a highly regulated area that could result in substantial liability. I've boiled most of the regulations into 2 basic traps you must avoid.

What is Marketing Copy?

Wikipedia defines "copy" as written material, in contrast to photographs or other elements of layout, in a large number of contexts, including magazines, advertising, and book publishing. In advertising, web marketing and similar fields, copy refers to the output of copywriters, who are employed to write material which encourages consumers to buy goods or services.

Web copy has one major advantage over offline copy - it is interactive. Hyperlinks provide you with powerful tools to lead a potential customer through a pathway designed by you which ultimately leads to a conversion to your call to action.
Trap No. 1: Failure To Substantiate Claims Before Publication

When you write your own marketing copy, you necessarily make certain "claims" - statements upon which a consumer may reasonably rely in making a purchase decision. In so doing, you're facing another legal pitfall.

Legally, claims are extremely important. The Federal Trade Commission (FTC) Act, 15 USC Sec. 41-58 and accompanying regulations prohibit "unfair or deceptive acts or practices". Unfair or deceptive acts or practices include claims that are not substantiated before the claim is publicly disseminated.

So review your ads carefully, and be sure that you can substantiate and back up your ad claims.

Here are some examples of claims and the related challenges regarding substantiation and back-up:

- If you claim "best value", understand that it's a promise that is very broad in scope - essentially, you're promising that your offer is worth more than the asking price - if you're going to make this claim, you'd better provide the proof on your site.

- If you claim "we're no. 1", you need to be very specific regarding how you determine no. 1 - no. 1 at what? - in gross sales, in sales growth for a specific period, in the number of widgets sold?

- If you claim the "latest and greatest", "next generation" or words to that effect, you should substantiate how the claim is true - explain
specifically how you justify the claim in relation to other competitive products on the market.

- If you claim "user friendly" or "easy-to-use", you need to be specific regarding substantiation of specifically how much time a certain task routinely takes, exactly which steps are automated, etc.

- If you offer a "risk-free guarantee", understand that even a free evaluation is not completely risk-free because the evaluation takes time for the customer to evaluate - time is money, so-to-speak, so a better approach is to promise an unconditional refund, no questions asked.

**Trap No. 2: Avoid Untrue And Deceptive Claims**

In addition to substantiating claims before making them, be careful not to make untrue or deceptive claims. Certain types of claims should be avoided altogether, including:

- never claim that you have a cure for anything - not even large drug companies with products that have been the subject of years of testing will make such a claim, so you shouldn't either;

- never specify a level of revenue or profits that a user will achieve, even if you or another purchaser has achieved a specific level of revenue or profits - remember the old adage, "your mileage may vary";

- never promise specific results - again "your mileage may vary".
The FTC has special rules governing any use of the term "FREE" (or similar words to that effect), which the FTC believes is frequently used in an untrue or deceptive way.

Similar words to "free" include:

- Buy 1-Get 1 Free;
- 2 for 1 Sale; and
- 50% off with the purchase of 2.

According to the FTC:

"[t]he public understands that, except in the case of introductory offers in connection with the sale of a product or service, an offer of 'Free' merchandise or service is based upon a regular price for the merchandise or service which must be purchased by consumers in order to avail themselves of that which is represented to be 'Free'. In other words, when the purchaser is told that an article is 'Free' to him if another article is purchased, the word 'Free' indicates that he is paying nothing for that article and no more than the regular price for the other. Thus, a purchaser has a right to believe that the merchant will not directly and immediately recover, in whole or in part, the cost of the free merchandise or service by marking up the price of the article which must be purchased, by the substitution of inferior merchandise or service, or otherwise."

**Conclusion**

In summary, be aware that what you say in your marketing copy is heavily regulated. You need to be careful not only to substantiate ad claims before you post them to your site, but also use certain key terms with great care so as not to mislead or deceive consumers.
Appendix 11

Beware of Unintended Warranties If You Write Your Own Product Descriptions

If you're like most small ecommerce businesses, you'll write your own product/service descriptions. In doing so, you will encounter a legal pitfall unknown to most... you may be creating unintended warranties that could result in substantial liability.

How can this be? How can you unwittingly create a warranty for which you will be held legally liable?

Uniform Commercial Code Warranties

The Uniform Commercial Code (UCC) is a collection of state laws that are relatively "uniform" from state to state. These laws govern the sale of goods, among other things.

In order to understand how you may create an unintended warranty under the UCC, first you need to understand that there are 2 basic kinds of warranties:

- implied warranties; and
- express warranties.
Implied warranties are created under state law. They are unwritten promises that a product will, at the time it is sold, meet certain minimum conditions, such as:

- be fit for a particular purpose; and
- be generally of merchantable quality.

The UCC provides that you automatically make the implied warranties listed above for products, unless you properly disclaim them. So, if you want to avoid these unintentional implied warranties, you must disclaim them in both your Terms of Use and in your Customer Agreement.

Express warranties are promises that are explicitly offered to a purchaser, whether they appear in advertising, a formal contract or certificate, or some other form.

The most likely way to create an unintended express warranty is to provide a demo or a product sample on your website. The UCC provides that a demo or product sample would create an express warranty that your products conform to the demo or sample. You may, however, disclaim these warranties. So, again, if you want to avoid these unintentional express warranties, you must disclaim them in both your Terms of Use and in your Customer Agreement.

**Limiting Warranties**

So, the lesson regarding warranties is that your objective should be to limit all warranties to express warranties where you control the terms and conditions by your carefully worded clauses. Important points to cover with express warranties include:
• the warranty period - how long does the warranty last (start with 90 days from purchase and work from there);

• specify the standards for performance (these should be objective, such as conformity with the user manual); and

• what is the remedy for warranty breach? (repair or replace, at your option).

All other warranties, both express and implied, should be disclaimed. That's the purpose of standard warranty disclaimers such as this one which is intended for use in your Terms of Use:

"EXCEPT AS MAY BE PROVIDED IN ANY SEPARATE WRITTEN AGREEMENT SIGNED BY THE PARTIES OR SEPARATE AGREEMENT ORIGINATING FROM THIS SITE, THIS SITE AND ITS LICENSORS SPECIFICALLY DISCLAIM, TO THE FULLEST EXTENT PERMITTED BY LAW, ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, RELATING TO THIS SITE OR PRODUCTS, SERVICES AND/OR CONTENT ACQUIRED FROM THIS SITE, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, COMPLETENESS, TIMELINESS, CORRECTNESS, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE."
Conclusion

We all like surprises from time to time... but not with unintended warranties. Unintended warranties can result in substantial liability for your website business, but they can be avoided altogether if you take the proper precautions.
Appendix 12
Beware of Human Intervention With Online Contracting - 2 Costly Mistakes To Avoid

The law of online contracting has become fairly well settled. This is good news for ebusiness sites with Membership Agreements, Subscription Agreements, Terms of Sale, SaaS Agreements, Content License Agreements, and the like.

Online contracting with click-wrapped agreements -- where the user indicates agreement by clicking on I AGREE -- will usually result in an enforceable contract if 5 simple rules are followed:

- conspicuous presentation during registration process;
- reasonable notice of the existence of contract terms;
- unambiguous manifestation of assent;
- opportunity to review contract terms, and
- opportunity to print agreement.
The above rules for online contracting are a relatively simple recipe for success. Recent cases suggest that if ebusinesses add human intervention to the online contracting process, rather than enhancing the enforceability of contracts, the exact opposite is likely to occur -- an unenforceable contract... and as a result, an ebusiness which is not protected from liability with contractual disclaimers and limitations of liability.

**The Feldman Case**

In the case of *Feldman v. United Parcel Service, Inc.*, No. 06 Civ.2490 (S.D.N.Y., March 24, 2008), Feldman used a kiosk inside a UPS retail outlet to contract for the shipment of a diamond ring which was later lost in shipment. The ring was valued at $57,000, but UPS' shipping contract clearly prohibited the shipment of items valued in excess of $50,000 in its Tariff Agreement.

The kiosk presented a Terms of Service link that pointed to a pop-up window which advised that:

- the UPS Tariff Agreement governed all shipments, and

- the Tariff Agreement could be obtained from an on-premises UPS agent, or from the UPS website (the URL of the home page was given, but there was no link specifically to the Tariff Agreement).

Feldman took up the matter with a UPS counter agent who agreed to ship the ring, despite knowledge that the ring was valued in excess of $50,000.

After the ring was lost, Feldman sued UPS for the value of the diamond ring. UPS moved for summary judgment (dismissal of the suit as a matter of law).
The Reynolds Case

In the case of Reynolds v. Credit Solutions Inc., No. 07-AR-1516 (N.D. Ala., Feb. 26, 2008), Reynolds purchased Credit Solutions' debt settlement services online with the assistance of a Credit Solutions agent. The transaction was initiated by a telephone call during which the agent advised Reynolds that the contract could be completed online.

Reynolds contracted online, and the telephone call continued during the online contracting process. Credit Solutions' recording of the call indicated clearly that the Credit Solutions agent hurried Reynolds through the online contracting process. Reynolds clicked on the YES - I CONSENT" button after only about 30 seconds to review the 8-page agreement.

Reynolds later sued alleging failure to provide the services contracted for, and Credit Solutions moved to dismiss the suit as a matter of law, or in the alternative, to compel arbitration.

Conclusion - Case Results And Lessons Learned

Both Feldman and Reynolds prevailed in their actions and successfully defeated the contracts at issue.

In the Feldman case, the court ruled in favor of Feldman stating: "'[t]hese facts, if proved, implicate a substantial face-to-face communication, suggesting that the surrounding circumstances might have prevented the plaintiff from having adequate notice of the terms of the Tariff."

In the Reynolds case, although the case was decided on other grounds, the court expressed concern over the contracting process, as follows:
"However, the court notes, as an aside, that someone who reads with the speed of a Jesse Owens in the 100 yard dash could not read the contract displayed on Picard's (plaintiff's) computer screen in 30 seconds particularly with Englert (defendant's agent) salivating on the other end of the line."

The lessons learn can be boiled down to this: human intervention in an online contracting process is generally a bad idea. It opens the door to issues that a customer can use to defeat the contract. I'm sure that the defendants in the 2 cases discussed above assumed incorrectly that human intervention would enhance the online contracting process, but for the reasons indicated, the result was just the opposite.
Appendix 13

Do You Own - And Control Your Domain Name? You May Be Surprised!

All too often, website owners are lax in nailing down ownership and control of valuable domain names, and as a result, are often required to litigate these issues costing them thousands. The case of Dawson v. Brandsberg illustrates these costly mistakes and how to avoid them.

Dawson v. Brandsberg - The Facts

The dispute was between a website operator and developer regarding rights to a domain name that consists of the operator's name: "robertedawson.com". Plaintiff Dawson and his real estate firm (the website operator) hired Defendant Brandsberg (the website developer) to develop a website. A key fact is that there was no written agreement regarding possession or use of the domain name.

Other important facts include: (i) Plaintiffs requested Defendant to register the domain name at issue; (ii) Defendant developed the website associated with the domain name; and (iii) Plaintiffs paid for the initial registration of the domain name, plus development, hosting, and maintenance fees for the website.
Eventually, the business relationship soured, and the Plaintiffs sought to transfer the domain name and the website to another internet service provider. The Defendant refused to transfer the domain name and the website, and essentially held the domain name hostage.

**Dawson v. Brandsberg - The Decision**

Dawson brought suit against Brandsberg in the U.S. District Court in Virginia under the Cyberpiracy Provisions of the Lanham Act, Section 43 (d), 15 U.S.C. 1125(d). Dawson v. Brandsberg, 2006 WL 2915234 (W.D. Va. Oct. 10, 2006). Plaintiffs argued that the federal cyberpiracy prevention statute was applicable, and that it protected the domain name and imposed liability for a bad faith registration with the intent to profit from the registration. Plaintiffs also argued that it had a non-exclusive, implied license to use the domain name, given that Plaintiffs had paid for registration, development, hosting, and maintenance of the website.

Defendant Blandsberg argued that (i) Plaintiff's name was not a proper trademark because it was not distinctive at the time of registration of the domain name, (ii) Defendant had registered the domain name and developed the website with the intent to sell it to Plaintiff at a later date, and (iii) Plaintiff had no copyright or implied license in the website.

Defendant Blandsberg filed for a motion to dismiss most of the counts of the suit. The Court ruled in favor of Plaintiff Dawson denying the motion. The Court seemed to rely heavily on Plaintiffs' arguments regarding the implied license, stating "Even assuming that Brandsberg created the website, if Plaintiffs have no license to use the website or domain name, the creation would be valueless".
Conclusion: Lessons Learned

Don't rely on oral agreements; get it in writing! Provide not only for ownership of the website, but also of the domain name.

Provide that your domain name be registered in your name, not in the name of the vendor.

Also, note that control over the domain name is very important, and control goes with knowledge of the ID and passwords to the domain name account with the Registrar. So to maintain control, be sure to change the password so that you are the only one who has access to the administrative controls for your domain name at your Registrar's site.
Top 7 Gotcha’s That Can Shut Down Your Online Business
Appendix 14

Website Terms of Use: Are Yours Enforceable? Does It Matter?

Clients frequently ask me, "click-wrapped", "browse-wrapped" -- what do these terms mean? Are they the typical legal mumbo jumbo?

Your Customer Agreement (often called a Subscription Agreement, Membership Agreement, or SaaS Agreement) is a so-called "click-wrapped" agreement because your customer indicates agreement by clicking on an I AGREE button. For this reason, click-wrapped agreements are usually legally enforceable provided they are presented correctly.

Your website's Terms of Use govern all visitors to your site -- both casual visitors and registered customers. Terms of Use are typically referred to as "browse-wrapped" agreements because there is no requirement to click an I AGREE button. So, the question I’m often asked is... since the Terms of Use do not require a click, are they legally enforceable? And if not, why have them on the site?

So, the question is... since the Terms of Use do not involve an affirmative action such as a click to indicate agreement, are they legally enforceable? And if not, why have them on the site?
A recent case involving a bot's repeated access to Southwest Airline's site provides some insight into the answer to the first question -- are browse-wrapped agreements enforceable?

**The Airline "Bot" Case**

In the case of Southwest Airlines v. BoardFirst, LLC, No. 3:06-cv-00891 (N.D. Tex. Sept. 12, 2007), Defendant BoardFirst utilized a software "bot" to assist passengers of Southwest Airlines to book the popular "A" group boarding passes.

The BoardFirst.com site utilized the "bot" software to book Southwest's customers for a fee, despite Southwest's Terms posted on its site that "use of the Southwest websites constitutes acceptance of our Terms and Conditions". Clicking on the Terms And Conditions link sends the user to Terms which authorized use of Southwest's site "only for personal, non-commercial purposes". Southwest's Terms did not require a click on an "ACCEPT" or "I AGREE" button -- hence, the Terms were of the browse-wrapped variety.

Southwest sent two cease and desist letters to BoardFirst, citing its Terms and demanding that BoardFirst cease its activities in breach of the Terms. BoardFirst continued its actions, and Southwest sued.

**Were Southwest's Browse-Wrapped Terms Enforceable?**

The Court noted that the validity of a browse-wrapped license turns on whether a website user has actual or constructive notice of the site's terms and conditions prior
to using the site. There was no dispute that BoardFirst had actual knowledge after receipt of Southwest's two cease and desist letters. The Court ruled that Southwest's Terms were enforceable against BoardFirst.

**Conclusion**

Note that the Court's ruling stands for the proposition that browse-wrapped agreements are enforceable only if there is actual or constructive notice of the terms. This ruling is consistent with prior cases involving similar facts. Because few if any ecommerce websites provide actual or constructive notice prior to use, it follows from this reasoning that most are not enforceable as contracts.

I'm often asked -- if Terms of Use are not legally enforceable in the absence of specific evidence of actual or constructive notice, what is their value?

One compelling reason for Terms of Use in ecommerce websites is that they usually provide various legal notices that are required by law for which agreement is not required. For example, if your site uses a blog, in order to qualify for the "safe harbor" from copyright liability, a specific notice is required, and a good place for it is in the Terms of Use.

Other notices that you must have on your site are certain legal disclaimers for which no agreement is necessary. Again, your Terms of Use is a good place for these disclaimers.

So, even though Terms of Use as typically used are not enforceable as a binding contract, they do provide a place for essential legal notices. And for this reason, Terms of
Top 7 Gotcha’s That Can Shut Down Your Online Business

Use serve an indispensable function on your ecommerce website.
3 Tips To Avoid Liability For Actions of Your Online Resellers

Recent case law confirms once again: if online agreements are presented properly to end-users, they're legally enforceable.

This continuing trend is good news for websites that contract with registered users though SaaS Agreements, Membership Agreements, Subscription Agreements, Terms of Sale, Content License Agreements, and the like.

Why? Among other things, this means that important legal disclaimers and limitations of liability are legally enforceable.

But what about liability exposure arising out of customer contracts entered into by your resellers? Are you liable for actions of your resellers?

The Direct Revenue Case

In the case of People v. Direct Revenue, the New York Attorney General in 2008 attempted to nail Direct Revenue for its distribution of software that served pop-up advertising software on consumers' computers.
Direct Revenue is in the advertising business. Its software client serves pop-up advertisements to consumer's computer screens through the Internet. Direct Revenue does not charge fees to consumers. Instead, it charges fees to the companies whose products it advertises.

It's interesting to note that one line of attack by the New York Attorney General focused on Direct Revenue's "click-wrapped" (where the user clicks on "I ACCEPT") end user license agreement (EULA) and Direct Revenue's alleged deceptive and illegal practices. The court granted Direct Revenue's motion to dismiss the claims noting that sufficient disclosure was given in the EULA, and the required elements for an enforceable agreement were followed.

Having failed with its first line of attack, New York's additional line of attack focused on the customer agreements of Direct Revenue's resellers in an attempt to hold Direct Revenue liable. The result was the same as with the EULA -- Direct Revenue was held not liable.

New York conceded that Direct Revenue's resellers were independent contractors rather than agents. Generally, a principal is not liable for acts of an independent contractor due to the lack of control over how the contractor's work is performed. In addition, the court noted that Direct Revenue's software distribution agreement required its distributors to obtain consent of consumers consistent with the EULA and prohibited distributors from holding themselves out as agents of Direct Revenue.

New York argued that Direct Revenue should be liable because its servers interacted with the consumers'
computers in the software installation process. The court pointed out that participation in installation was not enough for liability in the absence of participation in deceptive conduct that induced the installation.

Finally, New York argued that Direct Revenue should be held liable for the actions of its resellers on the ground that Direct Revenue ratified the conduct of its resellers. The court ruled that mere knowledge of consumer complaints was insufficient to impose liability on Direct Revenue, especially in light of the fact that when Direct Revenue had actual knowledge of a reseller misconduct, it took steps to remedy the problem.

**Conclusion** - 3 Tips To Avoid Liability For Actions of Resellers

Potential liability for acts of online resellers is a major concern of ecommerce businesses which use reseller networks.

The Direct Revenue case teaches us that ecommerce sites may not be held liable for actions of their resellers if these 3 tips are followed:

- if you transfer anything to a user's computer, require your resellers to obtain consent of end-users consistent with your EULA - this means consent in clear and easy-to-understand (not deceptive) terms,

- prohibit your resellers from holding themselves out as your agents, and
• if a reseller does engage in misconduct, take affirmative steps to deal with the situation, including termination, if warranted (particularly if the reseller's actions tend to indicate an agency relationship).

These 3 tips won't guarantee that you have no exposure, but they'll go a long way to protecting you from liability for actions of your resellers.
Appendix 16

Are Non-Clickers Bound By Your Online Customer Agreement?

It's well settled that website click-wrapped agreements presented on SaaS (Software as a Service) websites and ecommerce sites are enforceable against the clicker -- but what about users who access someone else's account without clicking to agree -- are they bound also?

The answer is critical to SaaS websites and ecommerce seeking to create binding agreements.

Binding Clickers To SaaS Agreements

The term "clickers" includes anyone who undertakes what attorneys call an action indicating affirmative assent to contract terms. With SaaS sites, this is usually achieved by requiring the user to click on an I ACCEPT button after presenting the user with conspicuous notice of contract terms coupled with the opportunity to review them. These agreements are typically referred to as "click-wrapped" agreements.

The most significant case regarding the enforceability of online, click-wrapped agreements against clickers is Specht v. Netscape Comms. Corp., a 2003 case in which the 2nd
Circuit Court of Appeals upheld a district court decision that Netscape's online agreement was not enforceable. By holding that the agreement was unenforceable, the reasoning of the case provided specific guidelines for enforceability.

Three additional cases regarding clickers - the Register.com case and two Ticketmaster cases - when taken together with the Specht case, make it clear that courts are most likely to enforce online agreements where the user gives express to assent to conspicuous contract terms. Express assent is usually given by clicking on an I ACCEPT button.

**Binding Non-Clickers To SaaS Agreements**

The term "non-clickers" includes users who access the account of a clicker without themselves clicking to agree. Recent cases suggest that non-clickers may also be bound to the contract terms.

The 2009 case of Burcham v. Expedia, Inc. involved a suit brought by Burcham (an attorney) against Expedia based on Burcham's use of the expedia.com website to book a hotel reservation. Burcham based his suit on a Missouri consumer law claiming that Expedia knowingly misrepresented the amenities for his hotel room.

Expedia demonstrated that that Burcham's booking was made after the presentation of a legend stating: "By continuing on you agree to the following terms and conditions". The complete text of the agreement was presented under the legend, and in order to book a room, the "continue" button was required to be clicked.
Burcham argued that he didn't remember the agreement, and that he may have accessed the Expedia site from someone else's computer in his office who had established the Expedia account (i.e. someone else was the clicker). The Missouri U.S. District Court held that Burcham was bound by Expedia's agreement.

An earlier 2004 case reached a similar result. In Motise v. America Online, Inc., a U.S. District Court in New York held that a non-clicker's use of a clicker's online account with America Online was bound by the click-wrapped agreement, even though the non-clicker was not presented with, and did not assent to, the agreement.

The court ruled that the non-clicker was a sub-licensee of the clicker, and was therefore bound by all of the restrictions of the click-wrapped agreement. The court noted that any other conclusion would permit non-clickers to avoid online contract terms by simply having third parties establish online accounts for them.

**Conclusion**

The extent to which non-clickers are bound by SaaS agreements is critical to the viability of SaaS and ecommerce websites that depend on click-wrapped agreements to regulate the use of their sites and services. The cases cited above are only the beginning of the process of development of the rules in this critical area.

Expect more judicial refinement in the near future.
Top 7 Gotcha’s That Can Shut Down Your Online Business
Appendix 17

Is Your Online Customer Agreement Enforceable Even against Simba, The Agreeable Cat?

I thought I’d seen and heard it all in my Internet law practice, until a client referred me to an interesting article about a kitty cat named Simba that walked across a keyboard and clicked on an online, click-through agreement (also known as a “click-wrapped” agreement). The article is entitled “The Agreeable Cat”, by Ann Loucks (Google the title, and you can read it for yourself).

My client wanted to know whether the agreement was enforceable. My reply – against Simba the cat, or its owner who put Simba up to this?

After a chuckle, I thought the question really had merit, and this is my analysis.

The Specht Case

The most significant case regarding the enforceability of online agreements is Specht v. Netscape Comms. Corp., a 2003 case in which the 2\textsuperscript{nd} Circuit Court of Appeals upheld a district court decision that Netscape’s online agreement was not enforceable. By holding that the agreement was unenforceable, the reasoning of the case provided specific guidelines for enforceability.
Top 7 Gotcha’s That Can Shut Down Your Online Business

In the Specht case, Netscape's website developer designed its download page for Netscape's SmartDownload software with little regard for contract enforceability.

Netscape's download page provided a download button that triggered the download of the SmartDownload software. The only reference to a license agreement required the user to scroll to the bottom of the same web page which provided a link to the license agreement. Clicking on this link directed the user to another page which stated that use of the software was governed by a license agreement that required still another click before the user could read the contract terms.

The 2nd Circuit ruled that Netscape's agreement was unenforceable because of 3 deficiencies:

- the user did not have to click on an I ACCEPT button to indicate assent;
- the text on the web page accompanying the download did not clearly state that agreement was a pre-condition to use;
- the failure to provide "reasonable notice" of the existence of contract terms.

The Register.com and Two Ticketmaster Cases

Three additional cases – the Register.com case and two Ticketmaster cases – when taken together with the Specht case, make it clear that courts are most likely to enforce online agreements where the user gives express assent.
Express assent is usually given by clicking on an I ACCEPT button.

Now we get back to the facts of the hypothetical case involving Simba the cat. Is the online agreement “accepted” by Simba enforceable against its owner who created the elaborate system for Simba to “agree”?

We’ll leave enforceability against Simba out of our analysis, out of deference to the agreeable cat.

Simba’s owner believes she has agreed to nothing. She states: “The download begins and I have personally agreed to nothing”. In essence, she argues that since there is no express assent (by her), there is no binding contract.

Not so fast, according to Register.com, and the two Ticketmaster cases. These cases also stand for the proposition that absent express assent, assent may be inferred from proof that a defendant (i) had actual notice that use or access was conditioned on legal terms, and (ii) continued to use or access a site, service, or software after acquiring that notice.

**Conclusion**

In summary, the online agreement would be enforceable against Simba’s owner if she had actual notice of legal terms and her use continued after acquiring that notice.

More important than the specific facts and result of the hypothetical case involving Simba the agreeable cat, are the
fundamental principles that support virtually universal recognition that online agreements, provided they are presented properly, are generally enforceable, even in the absence of express assent -- a significant legal foundation upon which our Internet economy depends.
Appendix 18

Sex, Lies... And a Dumb Mistake Your Blog Website Can’t Afford

Does your website incorporate a blog or forum – where users may post text or files? If so, are you liable if your users post defamatory materials about someone else?

In 1996, Section 230 of the Communications Decency Act (Section 230) came to the rescue of “interactive computer services” by overruling prior case law that would hold websites liable. But Section 230 is not absolute. Interactive websites may still be liable as the May, 2009, Ninth Circuit case of Barnes v. Yahoo, Inc. illustrates.

Sex And Lies

The case of Barnes v. Yahoo involved salacious facts centering on the aftermath of a break-up between plaintiff Cecilia Barnes and her boyfriend.

After the break-up, Barnes’ ex-boyfriend created fictitious profiles for her on a website operated by Yahoo. Included were nude photos, plus offers for sex. To make matters worse, he also provided her email address, physical address, and work phone number. All this resulted in Barnes receiving emails and calls with the expectation of a sexual liaison.
The Dumb Mistake

After Barnes’ four separate emails to Yahoo demanding the removal of the objectionable materials did not result in their removal, Barnes received a call from an executive at Yahoo. Barnes alleged that the executive promised to “take care of it”. Barnes further alleged that she relied on this promise and took no further action to remove the objectionable materials.

You guessed it – Yahoo failed to remove the objectionable materials, and after two months, Barnes filed a lawsuit against Yahoo.

Yahoo claimed complete immunity under Section 230(c)(1), and the trial court agreed by dismissing Barnes’ suit.

The Ninth Circuit Appeal

Barnes appealed to the Ninth Circuit Court of Appeals, arguing that Yahoo’s failure to make good on its promise took Yahoo out of the protection of Section 230.

The essence of Section 230 is that it removed an “interactive computer service” such as the Yahoo website from “publisher” liability for materials posted by a user. “Interactive computer services” include websites that offer interactive services such as blogs, forums, and listservs. As a result of Section 230, website publishers are treated differently from publishers in print, TV, and radio.

The Ninth Circuit agreed that Yahoo’s failure to make good on its promise took Yahoo out of the protection of Section
230(c)(1). Essentially, the promise was held to be an act separate and distinct from Yahoo’s role as an online publisher, and therefore, this departure from the role of publisher would not be immunized. In short, this decision illustrates that the Section 230 protections for interactive websites is not bullet-proof.

Conclusion

The ruling in Barnes v. Yahoo does not diminish the immunity provided to interactive websites by Section 230, provided that the website does not venture out of its role as publisher. The lesson from this case is that explicit promises to remove objectionable materials may well lead to liability for failure to make good on the promise.

One additional take-away is that all interactive websites should review their Terms of Use to insure that there is no provision that could be construed as a promise or guarantee for a specific response to a complaint by a user.
Top 7 Gotcha’s That Can Shut Down Your Online Business
Appendix 19

Your Online Customer Agreement - Which End-User Agreement Approach is Right For You?

If you offer software as a service (SaaS), your choices among contracting approaches for users include an electronic, click-wrapped agreement or a more traditional paper-based, signed agreement – or even a hybrid of these two approaches.

How do you decide which approach is right for you? What are the factors to consider?

Click-Wrapped Agreement Approach

With the click-wrapped agreement approach, the agreement is presented to the user as part of the online registration process, usually in a scroll box configuration. The user indicates assent to the agreement by clicking on an I ACCEPT button.

Click-wrapped agreements are usually utilized in one or more of the following circumstances:

- relatively low price point service, and/or
service that is tailored for the small businesses or consumer markets as distinguished from the corporate market.

The advantages of the click-wrapped agreement approach are:

• simplicity – the agreement is presented online automatically, and the process is relatively simple and easy;
• no negotiation of contracts – it’s a take-it-or-leave-it approach;
• no contract administration headaches – the agreement is the same for everyone and there are few contract administration tasks; and
• a relatively fast sales cycle due to the factors listed above.

The disadvantages of the click-wrapped agreement approach are:

• you’ve got to follow the applicable case law regarding the contracting process, or it won’t be enforceable;
• some users that do not agree with a specific contract term may not do business with you; and
• the corporate market may require more comprehensive contract terms and the opportunity to negotiate them.

Traditional Paper-Based, Signed Agreement Approach

With the traditional paper-based, signed agreement
approach, the agreement is presented to the user in paper form. It’s almost always negotiated, and it’s signed by both parties to indicate assent to the agreement.

Traditional paper-based, signed agreements are usually used in one or more of the following circumstances:

- relatively high price point service, and/or
- service that is tailored to the corporate market as distinguished from the small business or consumer markets.

The advantages of the signed agreement approach are:

- you have the opportunity to negotiate certain terms and conditions that may cause some users to go elsewhere, and
- you have the opportunity to present terms and conditions that the corporate market expects to see.

The disadvantages of the signed agreement approach are:

- complexity – the process is relatively complex and difficult;
- negotiation – a written agreement is an open invitation to negotiate and you’ll probably require the services of an experienced attorney;
- contract administration headaches – differences in negotiated terms and conditions require administrative attention; and
- a relatively slow sales cycle due to the factors listed above.
One key point to keep in mind – despite the disadvantages of the signed agreement approach, you may just have to use it if your primary market is the corporate market. As a general rule, the corporate market expects to see a written agreement with the opportunity to negotiate. If this is the case with your SaaS service, your market will dictate your contracting approach for you.

**The Hybrid Approach**

A hybrid approach – where both approaches are used – may be a way to avoid some or all of the disadvantages of click-wrapped agreement approach and the signed agreement approach.

With the hybrid approach, the click-wrapped approach is used as the default approach. However, the click-wrapped approach may be supplemented with the traditional paper-based, signed agreement approach for corporate users that insist on a comprehensive agreement the opportunity to negotiate.

**Conclusion**

Choosing the right contracting approach is vital to the success of an online business. The key is successfully addressing what your market expects or will bear, while reducing or eliminating as many contracting disadvantages as possible.
Appendix 20

How To Avoid FTC Biz Op Regulation

Effective on March 1, 2012, the FTC’s new Business Opportunity Rule (New Biz Op Rule) became effective.

The Biz Op Rule applies to a specific type of offer defined as a “Business Opportunity” (Biz Op).

The FTC’s objective with the New Biz Op rule was to make it very tough to make legally compliant Biz Op offers, particularly Biz Op offers that make earnings claims.

Because the New Biz Op Rule imposes numerous, detailed requirements, Internet marketers and online entrepreneurs should not offer Biz Ops. Even with careful attention to all the requirements, it would still be relatively easy to inadvertently cross the line into non-compliance, and therefore huge exposure to liability. In a nutshell, offering Biz Ops is a very high risk activity that should be avoided altogether.

Biz Op Defined

The New Biz Op Rule stipulates three elements that must be satisfied for an offer to be a Biz OP.
1. Solicitation For New Business Opportunity - a seller solicits a prospective purchaser to enter into a “new business” (i.e. a new line or type of business that the prospect is not currently engaged in);

2. “Required Payment” By Prospect – the prospect makes a payment, meaning all consideration paid by the prospect to the seller or an affiliate for the right to obtain or commence the operation of the business opportunity;

3. Business Assistance – the seller (or someone recommended by the seller) provides any of the following types of assistance:
   - Locations for the use or operation of equipment or other devices paid for by the prospect;
   - Outlets, accounts, or customers; or
   - Buy back promises for goods or services provided by the prospect.

How To Avoid Biz Op Regulation

The way to avoid regulation as a Biz Op is to not satisfy one of the three elements of a Biz Op under the New Biz Op Rule. Remember, all three elements must be satisfied for a Biz Op to exist, so if you satisfy any two elements, but not three, you’ve avoided Biz Op regulation.

So, one way to avoid Biz Op regulation is to offer only educational and training services, and not offer a “new business”. The FTC stated specifically that “general business advice and training” services are not included in
the Biz OP definition. However, some of the typical offers by Internet marketers and online marketers may come close to crossing over from education and training to operation of a “new business”.

However, if you analyze the three Biz Op elements, elements 1 and 2 may be satisfied by some offers typically made by Internet marketers and online entrepreneurs. With many offers there are “grey areas” with elements 1 and 2, where there’s no way to determine with confidence whether you’ve satisfied the element or not.

- For example, the “new business” requirement of Element 1 does not mean a person who has never been in business. The “new business” could be satisfied by an offer to an experienced business person if the offer presents a new line of business to the prospect. Sellers generally have no way of knowing the present business status of prospects.

- Another example: The “required payment” requirement of Element 2 may be satisfied by indirect payments through a third party. Even if you split a product into a free part and paid part, you’ll still satisfy the “required payment” requirement if the paid part is a “practical necessity” for obtaining or operating the business opportunity.

So, due to the relative uncertainty regarding elements 1 and 2, the recommended approach is to focus on not satisfying element 3, thereby avoiding Biz Op regulation.
Avoiding Element 3

Element 3 should be your primary focus in avoiding Biz Op regulation.

The key is to avoid providing business assistance by not offering to provide locations (this applies primarily to offline businesses), outlets, accounts, customers, or buy back promises.

Remember, providing “general business advice and training” services is OK, but the prospect must be solely responsible for finding his/her own customers or other ways to monetize the purchase.

Conclusion

Offering Biz Ops is a very high risk activity that should be avoided altogether.

To avoid Biz Op regulation with confidence, understand the definition of Biz Op under the New Biz Op Rule, and be sure that you’ve not satisfied at least one of its three elements.
About Chip Cooper, Esq.

Law Practice

- Of Counsel, Jones & Haley, Atlanta
- Internet, Software and SaaS Attorney
- Intellectual Property Protection and Transactions
- Content, Software and SaaS Licensing and Distribution Transactions
- Website Legal Compliance
- Mergers & Acquisitions

Adjunct Professor, Software Law, Wake Forest University School of Law, 20 years
Education

- Wake Forest University, BA
- Wake Forest University School of Law, Juris Doctor
- University of Georgia, Terry College of Business

Martindale.com - AV Rating (highest peer rating)

Published Author

- *Law and The Software Marketer, How To Develop a Legal Protection Game Plan*, Prentice-Hall
- *Software Distribution, How To Develop a Successful Marketing Plan*, SoftChannel Press

Law Firm Website

- [http://www.corplaw.net/](http://www.corplaw.net/)

Online Legal Document Service Website

- [www.digicontracts.com/](http://www.digicontracts.com/)

For more information for Chip Cooper to appear as a speaker at your event or to present a webinar based on this book contact:

**Rich Wilens Webinars Management**

228-238-7573

**Chip Cooper**

Jones & Haley, P.C.
South Terraces, Suite 170
115 Perimeter Center Place
Atlanta, GA 30346-1238
770-664-8555

chip@digicontracts.com
Additional contacts:
LinkedIn: www.linkedin.com/in/chipcooper
Skype: chip.cooper.esq

More About The Author

Keith Okano
President, Bridgeway Software, Inc.

“I've worked with many attorneys over 30+ years in the software and technology business and overall Chip is the best. He is expert in his knowledge of software contracts and my trusted counsel not only helping us close business, but also in ensuring we have the knowledge needed to manage and develop our company according to our needs and desires.

Chip does this not by simply offering "data," but taking the time to know and to understand us. Therefore he offers us more than advice, it is wisdom. Chip is a key part of my advisory team and I look forward to working with him for many years (and if necessary many companies) into the future.”

Michael Gerster
President, WIKA Instruments, LP

“I have worked with Chip Cooper since the year 2000 and he is my expert for any and all contractual issues. I could not get it all done without him and appreciate his counsel and guidance.”
Maurizio Taverna  
CTO, Mylaensys, LLC

“I recently asked Chip to work on intellectual property, licensing, SaaS agreements and website legal compliance. I found Chip to be friendly, professional and a person to work with. I would recommend Chip to anyone looking for legal expertise to address the issues for legal compliance and protection.”

Klaus K. Obermeier  
Big Data scientist, NLP expert, Artificial Intelligence professional

“Chip is a no-nonsense attorney that helped us during an $11M forward triangular merger and negotiated a large cash component. He has a Colombo-style inquisitiveness that gets to the bottom of every deal. Great to have him on your side.”

Bill Needle  
Intellectual Property Attorney, Mediator, Arbitrator & Special Master

“I’ve known Chip as an attorney for over 20 years. Chip is a top notch SaaS attorney and software attorney who has a depth of knowledge not only of the law, but also of the software and Internet industry that’s reflected in his legal documents and negotiations. He has a knack for resolving complex legal issues in SaaS and software transactions from a business perspective.

Chip is also a BBQ connoisseur who has been my mentor as a fellow Certified BBQ Judge at several Memphis in May World Championship BBQ Cooking Contests.”
Alex Eckelberry
Technology Entrepreneur And Executive

“Chip is a world-class expert in a broad range of issues. He has worked with us many times on software contracts, IP and other issues. He is always fair in his pricing, and is a highly ethical man of real integrity. I would recommend him without hesitation.”

Tom Johnson
Owner, PaperSoft

“We've engaged Chip for our Software License Agreements for years. He's very knowledgeable and gets to the point quickly. He always does a great job.”

More Information
For more information for Chip Cooper to appear as a speaker at your event or to present a webinar based on this book contact:

Rich Wilens Webinars
228-238-7573
Richwilens1@yahoo.com
Code: Book1
www.richwilenswebinars.com
Share This Book

If this book has opened your eyes to legal gotchas that you absolutely, positively need to avoid, chances are this information would be valuable to your friends and colleagues as well.

So, do everyone a favor and share this book!

You may also share it on Facebook, Twitter, and other social networks.

If you have realized value from this information I’ve shared with you, please take a moment to review my book on Amazon. All of your feedback will help make any revisions (or potentially, a sequel) even better than the original.

Thanks for your time and attention, and best of luck as you travel the road to online success!