US Laws on Privacy, TOUs & Email Marketing:

Can You Comply?

2017

James C. Roberts III, Esq.

GlobalCapital

Global Capital **Strategic** Group | Global Capital **Law** Group PC

THIS IS NOT LEGAL ADVICE

For example,

1. You and we have not agreed to an engagement
2. We have not learned of, and examined, your particular situation--e.g., your facts

COMPLIANCE WITH US LAW?

Lawyers have a narrow view of "compliance"

We don't like to say that someone is "compliant" with applicable laws because

1. It's a factual question: courts
2. It's a jurisdictional question: What law?

COMPLIANCE WITH US LAW? (CONT'D)

3. Multiple levels: federal, state, court opinions
4. You can be sued by others
    - Even if you think your site has everything "required"
    - You fail to follow your own privacy policy

What about Google, Facebook & Yelp?

Spent tens of thousands on lawyers' fees on privacy.

They were not "compliant" with applicable US law.

To Be Compliant (with Your Privacy Policy) Is "Doable"* *IF* . . .

1. You have a privacy policy that follows state law (possibly California) for ***content*** of your policy and the ***use*** of the data ***(best practices)***
2. Your policy includes what is required for your type of business, e.g., e-commerce ***(state laws)***

**means you have a good chance*

To Be Compliant (with Your Privacy Policy) Is "Doable" *IF* . . .

3. You do what your policy says you will do ***(federal and state laws)***
4. You are responsive to your customers' concerns ***(good business)***
5. You are not sued—or at least you win ***(good fortune)***

PART 1: PRIVACY POLICY

Remember: It is *your* policy. Follow it.

RAISE YOUR HAND IF YOU AGREE THAT . . .

US law requires every website to have a privacy policy

No.

US law does *not* require every website to have a privacy policy.

WHY DOES (ALMOST) EVERY SITE HAVE A PRIVACY POLICY?

Because major market players require a privacy policy

- *California and other states require it*
- *Google, Apple & Facebook require it in their stores (and analytic tools, e.g., Google Analytics)*
- *There are* some *situations where federal law requires it*

. . . So (almost) everybody has a privacy policy

The US Approach: (primarily) Disclosure & Some Use Regulation

Two different things:

- *Disclosure* is what you say on your site
- *Use* is how you use the personal information you collect

Moving towards greater use restrictions but primarily evaluated on performance against your promises

THE TWO PRINCIPLES OF APPLICABLE *FEDERAL* LAW

1. True & Accurate ("not misleading")
   - *If you have a privacy policy then you must do what that policy says you will do*
   - *It must be truthful*
2. The more sensitive the information or the group, the higher the requirements or the risk of government intervention:
   - *E.g., children, finance, women, minorities, healthcare*

The *Use* of Data Is Also Subject to Law

- Using personal information for:
  - Emails, newsletters, mass mailings, behavioral ads
- Using personal information that discriminates
- Data breaches (US and federal laws)
- *Doing anything contrary to your privacy policy*

Basic Principle of State Data Laws

States are more protective of their citizens than the US (which is not a criticism)

- States will intervene if they believe that their consumers are being harmed
- Site location is (largely) irrelevant

Consumer protection statutes: Fraud protection

- Obligations of a site = disclosure
- E-commerce = regular commerce, e.g., return policies

YOU *MUST* HAVE A PRIVACY POLICY *IF* YOU COLLECT PERSONAL INFORMATION AND . . .

1. Children use your site
   - Because you target children
   - You know that children use your site
2. You collect personal information of California or Massachusetts residents (no matter where you are)
3. You are engaged in e-commerce (because you collect PII)
4. You collect (and/or use) sensitive information (or about special groups)

What Is Personal Information?

Basically, any information from which you could identify a user

- Including information that could identify the user when used with other information

Statutory definitions also specify PII

What Is Collecting?

Sites that have contact forms

- "Contact Us" forms with fields
- "Sign up for our newsletter"

But (probably) not if a user contacts you on her/his own

- Email
- SMS

You would be stupid if you used PII from email in a way that violates your own privacy policy

Are Cookies and Tracking Collecting PII?

Cookies are *probably* collecting PII

- Third parties your site uses, e.g., Google Analytics
- Advertisements on your site

SOME SPECIFICS: COPPA

Do you

1. Collect PII from children (which could be unintentional)
2. Follow COPPA guidelines for the online policy, e.g.
   - List all operators collecting personal information
   - Describe what personal information is collected, and how it is used
   - Describe parental rights
3. Notify parents directly and get their consent
4. Respect ongoing rights of parents to control PII

Other Privacy/Site Requirements

CalOPPA

- e.g., “Do Not Track”

California “Shine the Light”

- For companies larger than twenty, the “right to be forgotten”

SOPIPA

- Stricter requirements when students are your target

WISP (Massachusetts)

A Quick Look: CalOPPA

Among other requirements for your privacy policy:

1. A list of PII categories collected
2. Third parties with access to PII
3. A description of the process (if any) for a consumer to review and request changes
4. Policy change notice procedure described
5. Privacy policy effective date
6. “Do not Track” policy

From Data Privacy to Data Security

US and state laws now have breach notification requirements for data *security*

In sum: Your Privacy Policy Should Say

Who
What
Why
How
Others

Plus

Opt out
Changes
Effective date
Data breach notification

THE DETAILS

Who = Who you are

What = What you do with the data

Why = For what purposes?

How = How do you use the data to achieve those purposes?

Others = Who else has access to your data and for what purposes?

THE DETAILS (PART 2)

Plus

Opt out = I want to leave

Changes = How you notify them of changes

Effective date = When the policy *and the changes* take effect

Data breach notice = What happens and how you notify them

Do not Track = Do you (or anyone else) track beacons?

Other Advice: Don't Copy

Facebook and Google are under consent decrees with 20-year periods of supervision

Important Detail: Which Privacy Policy Version Applies When?

If you change your policy then:

- Not retroactive
- Opt-in/opt-out
- Archive and make available previous versions
- Data collected under a previous version is subject only to that version (unless they consent)

One More Detail: Privacy Policies are a *Policy*

We generally do not think it is a good idea to have your privacy policy as part of your TOU (an agreement)

- Means that if you violate your own policy then you could be subject to contract damages

IT'S NOT (ONLY) YOUR POLICY, IT'S YOUR CONDUCT

It's following your policy that really matters

- Yelp
- Facebook
- Google

It's Also Good Business

It's also good business to do the right thing

Customers like it

Regulatory agencies like it

Investors like it

And it's profitable

PART 2: TERMS OF USE

Terms of Use=TOU=

Terms of Service=TOS=

Terms and Conditions=T&C's=

End User License Agreement=EULA

They're all the same: an agreement between the company that owns the site and the user

Is a TOU Required?

A TOU is not required by law.
It is required by common sense and best practices.

Like any agreement, a TOU does (at least) one thing:

Limits your liability

State Law Governs TOUs

Your TOU should have all the elements* of an agreement

- Offer/acceptance (opt-in)
- Consideration
- Start date (usually some way to determine end date)
- Rights granted (i.e., their use of the site's content and features and functionality)

State Law Governs TOUs

- Obligations and consequences
- Liability sections (warranties, etc.)
- Dispute Resolution
- Choice of law and venue

*This is not a complete list

State Consumer Protection Laws (Usually) Apply

You'll need to comply with state laws on:

- Truthfulness & accuracy ("not misleading")
- Returns policy (usually of the state of the user)
- Auto-pay/pre-pay
- Other state-specific requirements

SOME E-COMMERCE ISSUES OF A TOU

If you are offering a service for payment (or e-commerce) then state laws (usually) apply on the following:

- Delivery of services/products
- Payment procedure and related terms
- Disclosure of all fees (e.g., S&H)
- Return procedure

OPT-IN/ACCEPTANCE

The trend is towards affirmative opt-in (and even double opt-in)

- "Access/use as consent" still generally valid
- The more "sophisticated" your site (e.g., e-commerce, financial services, healthcare), the stronger the case for affirmative opt-in (check a box)

Details: Rights Granted (Scope of Use)

No matter what your site provides, you should include

- Grant of right of use:
  - Access
  - Personal use
  - Use of data resulting from use of features/functionality
- Limits on that use
  - No copying/downloading
  - No other uses (reverse engineering)

Other Requirements: Auto-Renewal Disclosure

Federal and (some) state laws require clear disclosure and opt-in consent if there is auto-renewal (e.g., auto-pay, subscriptions, etc.)—and other limits

- ROSCA (Restore Online Shoppers Confidence Act)
  - No "negative option"
- California Automatic Renewal Law
  - Consent is conspicuous and before or in clear proximity to the signature line

We Also Like

"Contact us to discuss any terms. [However, customized changes may result in a different price.]"

Lessens risk of an "adhesion contract"

Part 3: Email Marketing

More complicated regulatory regime because of long history of state control of physical mailings ("direct marketing")

Email Marketing is About not Annoying Your Contacts

Major elements:

1. Get permission: express or implied
2. Be truthful
   - It's an advertisement and the subject line is accurate
   - It's you
3. Give the customer some control (opt-out, etc.)
4. Control others (third parties)

FEDERAL LEVEL: CAN-SPAM ACT OF 2003*

- Based on the principle of truthfulness & accuracy + "some" control by users
- Regulates both content and sending activities
- Includes criminal penalties for willful acts

**Controlling the Assault of Non-Solicited Pornography And Marketing*

CAN-SPAM Act Message Requirements

- Accurate
  - "From" lines
  - Relevant subject lines (not deceptive)
- At least one sentence in the email
- A legitimate physical address
- Obvious and operational unsubscribe mechanism below the body
- Identify it as an ad

CAN-SPAM Other Requirements

- Opt-out must occur within ten days
- Further use of emails limited to compliance
- No harvested emails
- No false IP addresses, etc.
- Identify it as adult content if included

Conclusion

Keep your customers happy
(and stay out of the press and out of court)

In Sum . . . For Your Privacy Policy

1. Be truthful, accurate and complete
2. Full disclosure is your best friend
3. Follow best practices
4. The more advanced your service, the more requirements (e.g., e-commerce, healthcare, women, children or minorities)
5. Give control to visitors
6. Do what you say you do

IN SUM . . .FOR YOUR TOU

1. It is an agreement
2. Include what is required in any contract
3. Make it easily understandable--language, fonts, etc.
4. Consider affirmative opt-in
5. If in e-commerce, follow state requirements on returns, reps & warranties, etc.
6. Content then specify rights and limits of use
7. If a subscription model with pre-pay, pay attention to requirements
8. You will be subject to state law—yours and/or your customer's

In Sum . . .Email Marketing

1. The rules are straightforward: Follow them
2. Be prudent: Don't overdo it
3. Monitor actions by third parties

COMPLIANCE?

Because US law is based primarily on disclosure and truthfulness, compliance *can* be achieved

- More than just "checking the boxes"
- Do what you say you will do
- Be prudent
- Be responsive to your customers

It’s not just the law. It’s good business.

THANK YOU

JAMES C. ROBERTS III

jcr@globalcaplaw.com

GLOBALCAPITAL

GLOBAL CAPITAL STRATEGIC GROUP | GLOBAL CAPITAL LAW GROUP PC