SABA
SOUTH ASIAN BAR ASSOCIATION
OF NORTH AMERICA

Advertising and Privacy Law Considerations for In-House Counsel

June 21, 2014
SPEAKERS

Jennifer Baumann
FTD Companies Inc.

Monique Bhargava
Winston & Strawn LLP

Rebecca H. Davis
Wal-Mart Stores, Inc.

Mona Thakkar
Volkswagen Group of America, Inc.

MODERATOR

Sanjana Sharma
UL LLC
Agenda

• Privacy Laws & Regulations

• Advertising Laws & Regulations

• Hot Topics in Privacy/Advertising Law

• Q & A
What Laws Regulate Privacy

CalOPPA

Beverly Song

STATE

Security/Breach

Health/Financial
What Laws Regulate Privacy

- CAN-SPAM
- TCPA
- TCFAPA
- Online Ads
- OTHER
US Approach

Notice

Choice
Expanding Definition of "Personal"

Sensitive:
- SSN, financial, health info

Identifiers:
- Names and addresses, phone numbers

"Other":
- Zip codes, location-based information

Behaviors:
- Online activities, mobile app usage

What's next?!
US: Aggressive Enforcement

- $22.5 Million
- $2.4 Million
- $800,000
- $15 Million
Complying with US and Non-US Law

- Comply with Highest Standard
- Regional Compliance
- Data Transfer-specific basis
The Anatomy of a Privacy Lawsuit

• Brought using deceptive trade practice allegations (FTC Act, state DPTA, Lanham Act)
  – Alleging deception or
    • Eli Lilly (FTC): You said you wouldn't share and you did, first privacy case, no damages
    • CollegeNET v XAP: you said you would only share with permission ($4.5 million jury verdict)
  – Alleging unfairness
    • Choice Point: It was fundamentally unfair to let an ID thief get credit report information ($15 million)

• Who brings: FTC, State AGs, plaintiffs class action attorneys, competitors
Agenda

• Privacy Laws & Regulations

• Advertising Laws & Regulations

• Hot Topics in Privacy/Advertising Law

• Q & A
Advertising = Any commercial speech intended to influence consumers and disseminated to the relevant purchasing public. Generally not editorial or informational speech which is protected under free speech principles.
WHO REGULATES ADVERTISING?

- Federal
- State
- Industry
- Consumers
Claims, Substantiation, and Disclosures

- Claims must be truthful and not misleading
- Claims must be substantiated before and during the time they are in use
- Claims that could be misleading should contain clear and conspicuous disclosures
What is a Claim?

Express Claim: • A claim that is literally made

Implied Claim: A claim that is made indirectly or by inference

• A claim that is made indirectly or by inference
Actionable Claims

- Literally falsity
  - False on their face.

- Literally true but misleading
  - Statements that are accurate but deceptive
Non-Actionable Claims

Puffery
- Claims that are so broad that consumers would not take them seriously, e.g., “world’s greatest,” “best in the universe,” etc.

Opinions
- Statements expressing an opinion rather than fact or that is unmeasurable
Elements of a False Advertising Claim

- Business made false or misleading statements about its own or another’s product;
- There is actual deception or at least a tendency to deceive a substantial portion of intended audience;
- The deception is material – likely to influence purchasing decisions;
- The advertised goods traveled in interstate commerce; and
- There is likelihood of injury to another company in terms of declining sales or loss of goodwill.
Agenda

• Privacy Laws & Regulations

• Advertising Laws & Regulations

• Hot Topics in Privacy/Advertising Law

• Q & A
DATA BREACH
DATA BREACH - Landscape

Victims
- Customers
- Companies
- Government
- Employees

Consequences
- Identity theft
- Financial fraud
- State secrets
- Trade secrets
- Criminal fraud

Tools
- POS Intrusions
- Web app attacks
- Insider privilege misuse
- More...

Perpetrators
- External
- Internal
- Business Partners
DATA BREACH – Implications

- Reputation
- Compliance
- Financial Cost
“Cyberthreat will post the greatest threat to our country.”
—FBI Director Robert Mueller
DATA BREACH – Mitigating Actions

- **Prevent**
  - IT Security Program
  - Compliance Assessment
  - Employee Training & Awareness
  - Access Controls
  - Business Partner Management Program
- **Detect**
- **Respond**
  - Cyber Insurance
  - Data Breach Plan
- **Recover**
DATA BREACH – Data Breach Playbook

- Team
- Investigative Protocols
- Scope
- Notifications
- Offerings
- Annual Tabletop
- Corporate Comm. Plan
- Internal Reporting/Tracking
- Privilege
SOCIAL MEDIA
SOCIAL MEDIA – Risk Areas

- Communications on behalf of the entity
- Communications reflecting upon the entity
- Communications/Interactions within the company
- Communications/Interactions emanating outside the entity
- Electronically stored information
## SOCIAL MEDIA – Policy Considerations

<table>
<thead>
<tr>
<th>Define Social Media and Scope of Policy</th>
<th>Establish Authorized Users for Company’s Social Media Accounts</th>
<th>Discuss Permissible Use (Encourage vs. Tolerate?)</th>
<th>Be accurate and professional; avoid false or misleading statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know your audience</td>
<td>IP / Confidentiality Considerations</td>
<td>Compliance with National Labor Relations Act</td>
<td>Compliance with terms of use for social media websites</td>
</tr>
<tr>
<td>Privacy rights of users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Articulate who can respond to negative posts, criticism</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SOCIAL MEDIA – Pitfalls to Avoid

- Social media & unlawful harassment (ex. inappropriate conduct among employees on social media)
- Policy cannot prohibit employee organizing, protests, reports of illegal activity, freedom of speech
- Sweepstakes and contests
- User generated content (post your story, post your pictures)
- Third party bloggers (need assignment/license of rights in content)
SOCIAL MEDIA – Additional Considerations

- Third party monitoring
- Internal Cross Functional Response Team
- Insurance
- Cyber attacks
LOCATION BASED TECHNOLOGIES
Location-Based Technologies

Cellular

GPS

WiFi
Location-Based Services

- Navigation & Travel
- Tracking & Geosocial
- Gaming & Entertainment
- Retail & Real Estate
- Advertising
- News & Weather
- Device Management
Disclosure to Third Parties - FTC Guidance

- March 2012- Privacy Report, Protecting Consumer Privacy in an Era of Rapid Change
  - If location data is collected and shared with third parties, entities should work to provide consumers with more prominent notice and choices about such practices.

- February 2013 – Mobile Privacy Report, Mobile Privacy Disclosures: Building Trust through Transparency
  - Just in time disclosure + affirmative consent
Issues Affecting Automotive Industry

- December 2013 – Senator Markey (MA) sent letter to 20 automakers focusing on automobiles’ potential vulnerability to hacking.

- January 6, 2014 – GAO Issues Report: In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers

- January 8, 2014 - Automotive Executive: "We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing. By the way, we don't supply that data to anyone."
  - Senator Franken further inquired into Ford’s practices
  - The Location Privacy Protection Act reintroduced - requires consumer consent before collecting location data and additional disclosures
General Privacy Considerations

• Consideration of Privacy Issue at Earliest Stage of Product Development

• Security of Data

• Timing and Sufficiency of Notice

• Data Minimization
Disclosure to Government

- Fourth Amendment: protects against unreasonable searches and seizures
  - United States v. Jones (U.S. Supreme Court 2012): The Government’s attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a search under the Fourth Amendment.

- Constitutional Right of Privacy in Location Data
  - Commonwealth v. Augustine (MA Supreme Judicial Court 2014): Commonwealth must obtain a search warrant to acquire historical cell site location information (CSLI) from a service provider for a particular cellular telephone; given its capacity to track the movements of the user, the individual has a reasonable expectation of privacy in his CSLI
  - State v. Earls (NJ Supreme Court 2013): Reasonable expectation of privacy in their cell phone location data under the NJ Constitution.
DO NOT TRACK
Agenda

• Privacy Laws & Regulations

• Advertising Laws & Regulations

• Hot Topics in Privacy/Advertising Law

• Q & A