Privacy for Broadcasters

Presented to

Texas Association of Broadcasters

David Oxenford
Ronnie London

What We'll Talk About—Privacy Laws that Grow With Technology

- Traditional privacy issues—issues that come up in newsgathering and on-air broadcasts
- Issues that arise with technology
  - Phone
  - Fax
  - Emails
  - Cell Phones and Texts
- New Media Issues
  - Issues with Personally Identifiable Information ("PII")
  - Issues with Data Security
- Future of privacy issues
  - How it may affect new media promises and opportunities

Traditional Privacy Torts

- Issues that come up in lots of “old media” applications—e.g. news gathering, covering live events, taking pictures of people, on-air discussions, advertising, etc
  - False Light
  - Publication of Private Facts
  - Appropriation of Name/Likeness
  - Intrusion upon Seclusion/Invasion of Solitude

Publication of Private Facts

- What to worry about? How can you get sued?
  - The facts must be private and not available to the public or taking place in a public place
  - Plaintiff must be identifiable
  - Publication must be highly offensive to a reasonable person

Appropriation of Names and Likeness

- Advertising issues
- Taking information about or the likeness or identity of a person and appropriating it for commercial purposes without permission
- Law suits brought under state laws
  - "Incidental use" not actionable (*e.g.*, person pictured among many in a crowd scene)
  - Nor is using publications about persons that are protected because they're newsworthy and republishing them in the form of ads to promote circulation/audience-share

Intrusion Upon Seclusion

- Wrongful intrusion into place or matter as to which the there is a reasonable expectation of privacy
- In manner highly offensive to a reasonable person as to cause shame, outrage, mental suffering, or humiliation to persons of ordinary sensibilities
- Where will this come up? Newsgathering, DJ stunts … use and disclosure of personal information to customize messaging or experience with media to recipient

Broadcast of Phone Conversations—FCC Rule § 73.1206

- Before recording a telephone conversation for broadcast, or broadcasting such a conversation simultaneously with its occurrence, a licensee shall inform any party to the call of the licensee's intention to broadcast the conversation
- FCC is very strict—lots of fines for recording calls, even voicemail messages, without permission
- Even recording someone saying hello before getting permission is an issue
- Exceptions—where the caller should know that that the call will be broadcast

Telephone Consumer Protection Act of 1991 ("TCPA")

- What does it cover?
  - Automated/Prerecorded Calls
    - Came to include text-messaging
  - Unsolicited Facsimile Advertisements
  - Telephone Solicitation and Telemarketing

Automated/Prerecorded Calls & Texting

- Big penalties for violations
  - Prohibited to cell phones—regardless of content, purpose, or whether B2B or B2C—absent prior express consent
  - Prohibited to residential numbers unless there is prior express consent, or an exception applies:
    - Not for commercial purpose
    - Commercial purpose but no unsolicited ad or sales pitch
      - FCC has specifically held this includes prerecorded message (and, by extension texts) that merely to invite a recipient to listen to or view a broadcast
    - Established Business Relationship
    - By or for non-profit tax-exemption organization
  - State laws may also apply

“Junk Fax”

- Lots of big FCC fines—plus private rights of action
  - Prohibits use of any fax machine, computer, or other device to send to a fax machine an unsolicited advertisement, unless—
    - recipient has given prior express invitation or permission or unsolicited ad is from a sender that has an “established business relationship”—or “EBR”—with the recipient;
    - the sender obtained telephone number of the receiving fax machine through permissible channels, *and*
    - the fax has a clear and conspicuous notice advising recipients of the right to “opt out” of future faxes from the sender
    - Requires creating and honoring an internal “do-not-fax” list
  - Header/first-page disclosures for all faxes (ads or otherwise)
  - Applies to both B2B and B2C
  - State laws generally preempted

Telemarketing/Do-Not-Call

- Governed both by FCC TCPA Rules, and FTC's Telemarketing Sales Rule adopted Under Telemarketing and Consumer Fraud and Abuse Prevention Act (1995), which provide largely parallel regulatory regimes
  - Compliance with National Do-Not-Call Registry (DNCR)
  - Compile/maintain/honor internal do-not-call list
  - Caller ID required and abandoned calls limited
  - 8 a.m. to 9 p.m. calling time restriction
  - Mandatory disclosures for calls
  - Special allowance for free over-the air broadcasters to tout upcoming programming should apply here as well
  - Prerecorded messages, cellular scrubbing still required
    - Plus, where calls is for sales purpose, FTC requires prior express written signed consent, plus automated opt-out (FCC is considering requiring same)
- Does *not* cover B2B
- State laws may also apply

Email: CAN-SPAM Act of 2003 & Rules

- Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM") & FTC implementing rules
  - Prohibit false or deceptive email headers ("to" & "from" fields) and subject lines
  - Require commercial email to be identified as ads
  - Require showing valid physical postal address in email
  - Require allowing recipients of commercial emails to opt out of future emails from sender, which must be honored in 10 days
    - Thus sets up an opt-out regime, and need to create and maintain an internal "do-not-email" list
- Authorizes FCC to regulate wireless spam
- Fines here too! (Though limited private cause of action)

CAN-SPAM Act & Rules (cont'd)

- CAN-Spam Act & implementing rules
  - Reach only emails with primary purpose of promoting or advertising commercial products or services
    - Applies to B2B and B2C
  - FCC regulates "mobile service commercial messages" to wireless domains, *i.e.*, emails to addresses assigned by wireless services (*e.g.* "@t-mobile.com")
    - Requires opt-*in* and special disclosures
    - Wireless providers must register domains with FCC, email senders must scrub against domain list
    - But TCPA rules govern text messages to wireless service subscribers via phone numbers

Online Privacy—In General

- No comprehensive privacy law in the United States
- Tradition in United States is that data collector, not the data subject owns and controls the data
  - Though there are restrictions on what service providers might be able to do in special role as gateways to communiction
- And with consent, all things are possible…

So, What's the Problem?

- Consumer Backlash; Unpredictable Consumers
- Privacy Policies; Privacy Defaults
- FTC Action; Consumer Protection Issues
- Invasion of Privacy Claims
- Special Issues
  - Kids
  - Location Based Services

The Children's Online Privacy Protection Act of 1998 ("COPPA")

- Operators of websites or online services that are for kids under 13 or that have actual knowledge they are collecting personally identifiable info from kids under 13 must notify parents and get "verifiable parental consent" before collecting, using, or disclosing the info

- "Verifiable parental consent" = methods reasonably calculated, in light of available technology, to ensure person providing is child's parent
  - Uses "sliding scale" mandating more reliable means for operators intending to disclose info to third parties than those using the info only internally

- Exceptions for contests, one-time contact, email-only in some contexts

Collection of PII & Behavioral/Targeted Advertising

- Collection of PII for a variety of purposes
  - "Loyal listener" clubs
  - Marketing your own goods/services
  - Sharing with advertisers
  - Online tracking for ad placement
  - Move to app-based environment leads to another vehicle for collecting PII, expansion to UDID and/or geolocation data
- Presently, still regulated under FTC standards (and state "little FTC" laws) for practices that may be unfair or deceptive
  - And, state enforcement and/or class actions can follow, or even precede FTC action

Collection of PII & Behavioral/Targeted Advertising

- A trade practice is deceptive if it “misleads” consumers and “affects consumers’ behavior or decisions about a product or service
  - “Material"—that is, important to a consumer's decision to buy or use the product; and
  - Likely to mislead consumers acting reasonably under the circumstances.
  - See: FTC Policy Statement on Deception (1983) http://www.ftc.gov/bcp/policystmt/ad-decept.htm

Collection of PII & Development of a Privacy Policy

- Must explain to visitors to websites and others from whom PII is collected, used and/or disclosed the relevant practices
  - Should be set forth in privacy policy in user-friendly, easy-to-understand terms

- Privacy policy basics:
  - What information will you collect
  - To what uses will it be put
  - To whom will it be disclosed
  - How to opt out
  - Where to direct inquiries

Collection of PII & Behavioral/Targeted Advertising

- Privacy by Design: In addition to general practices of having a privacy officer training staff, etc., companies should, design privacy into every product, service, and application with the same concern given to, for example, costs
  - Provide reasonable security for consumer data
  - Collect only the data needed for a specific business purpose
  - Retain data only as long as necessary to fulfill that purpose
  - Safely dispose of data no longer being used
  - Reasonable procedures to promote data accuracy

Collection of PII & Behavioral/Targeted Advertising

- Notice: Clear notices, ideally given to consumer in a less-burdensome, standardized format at a time and in a context when it is meaningful (i.e., when they are making decisions)
  - Emphasize transparency and comprehensibility
  - Strive for models that allow easy comparison with other firms' privacy notices.
- Simple choices: Graduated level of consumer choice depending on use.
  - "Commonly-accepted" uses, such as order fulfillment, service improvement, fraud detection, legal and law enforcement compliance, first-party advertising on the same platform, and possibly advertising by obvious affiliates, might be permitted without choice.
  - For almost everything else—first-party advertising through different media, third-party advertising networks, data collection by ISPs, collection of "sensitive information," and collection of any information about "sensitive users" like impulsive teens should all be subjected to a heightened level of choice—the level of protection afforded should be proportionate to data and risks involved
    - FTC advocates a "just-in-time" approach, in which company provides consumer with a choice at the point the consumer enters his personal data or before he accepts a product or service

Location-Based Services

- Where you are as PII
- Front edge of the issue just reaching us now with iPhone and Android hearings
- As media transition to app-based delivery of content, this stands to become more of an issue
  - Apps raise same issues as online collection of PII
    - Insofar as content is ad-supported, and/or ad space may be sold within app itself, collection of PII and tailoring move to the fore

Honor Data Security Promises

- Designation of an employee or employees to coordinate information security program
- Oversight of securing sensitive personal information collected
- Routine information-security risk assessments and establishment of safeguards against identifiable risks
- Deployment of available security defenses and other measures
- Monitoring, bookkeeping and record-keeping that demonstrate functioning and efficacy of program
- Reasonable steps to ensure third parties with which company shares sensitive information have in place sufficient measures to ensure sensitive data shared will be secured by third party

Chief Privacy Officer

- Information practices and privacy policies
- Privacy Oversight Committee
- Monitor laws, represent company
- Notice and consents
- Privacy training and orientation, sanctions for violations
- Track use of information, reviews security
- Track complaints

UGC & Anonymity

- CDA/§ 230 immunize websites from liability for information/content posted by a third party

- Injured parties may still seek to learn identity of posters of the information
  - Balances First Amendment right to speak anonymously against need to redress harm, under various factors, including:
    - Ability to establish a prima facie claim (generally a prerequisite)
    - Specificity of discovery request
    - Availability of alternative means to obtain the information
    - Central need for the information
    - Poster's expectation of privacy

What's on the Horizon

- Congress/FTC run out of patience waiting for self-regulatory regime they deem acceptable?
- Commerce Department gets into the act
- Privacy Bill of Rights
- Do-Not-Track
- Do-Not-Track Kids
- State laws (*e.g.*, California Do-Not-Track)

Overarching Practical Tips

- Consider adding a CPO, or at least assigning some CPO-like responsibilities
- Maintain (or create) a good working relationship between legal and marketing
- Track the way customer data is managed; ensure that those that opt-out get opted-out in the system
- Make sure you know what data you will collect from consumers, and what uses you could possibly make of that data—and disclose that in your privacy policy
- Make the disclosures easy to find and understandable
- Establish system of internal reporting and checks and balances to detect and solve problems early, before they snowball
- Monitor third-party vendors, partners and affiliates
- Beware of the “creeped out” factor. Privacy concerns typically arise where the intrusion seems akin to dystopian science-fiction

David Oxenford
davidoxenford@dwt.com
202-973-4256

Ronnie London
ronnielondon@dwt.com
202-973-4235

Our Blogs:

www.broadcastlawblog.com

www.privseclaw.com