Caveat Venditor (Seller Beware) — State Law and Other Marketing Traps for the Unwary

By Jim Snell and Courtney Smith, Bingham McCutchen

Introduction

Advances in technology provide businesses with unprecedented opportunities to market products and services to customers through phones, mobile devices, applications, email and the Internet.

A patchwork of often inconsistent state, local and federal consumer protection laws, however, governs such marketing activities. Such laws often include private rights of action, sometimes with statutory penalties and awards of attorneys' fees, that allow individuals to file claims, including class action lawsuits. Moreover, given the challenge of applying such laws to developing technologies, courts have grappled with the proper construction of such laws – making application sometimes unpredictable. Further, the proliferation of mobile technology and nature of the Internet make it difficult to target marketing to a specific jurisdiction and thus it is often unclear which laws might be alleged to apply to marketing conduct.

The following broadly summarizes the marketing laws of which businesses should be aware. The list is not comprehensive, but the goal is that readers will be better able to spot issues related to specific marketing practices for further investigation.

Telemarketing and Texting

Existing laws address various aspects of telemarketing, including direct telephone solicitation and mobile texting.

A. Telemarketing and Do-Not-Call Laws

The federal Telephone Consumer Protection Act of 1991 ("TCPA") imposes restrictions on the use of autodialers and prerecordings to send unsolicited advertisements, and prohibits calls to phone numbers placed on a national Do-Not-Call list. Businesses who contact consumers without consent using autodialing systems may be liable under the TCPA. The TCPA

has been interpreted to apply to mobile texts as well as phone calls (see below). A private right of action exists as well as enforcement by regulatory agencies like the FTC and FCC, and state Attorneys General. The FCC announced in mid-February 2012 that it is tightening rules against "robocalls," requiring telemarketers to obtain customers' express consent before initiating sales calls through automatic dialing. The new rules also limit "dead air" calls, and require telemarketers to implement an automated, interactive mechanism that allows consumers to opt out of additional calls by pressing a button during a robocall.

Similar state laws also exist. With regard to telephone calls, for example, California generally allows consumers to add phone numbers to the national Do-Not-Call list, and to file claims when businesses call them after numbers have been on the list for at least 31 days. Massachusetts also allows a private right of action for an injunction or recovery of damages up to $5,000 for knowing violations. The Massachusetts Consumer Protection Act allows for up to treble damages where claims of knowing violations are not settled within 30 days. Other states, such as Michigan and Texas, also allow private rights of action for do-not-call violations. Even where such statutes do not expressly apply to text messages, as discussed below, plaintiffs may claim that they should be interpreted broadly enough to cover text messaging.

Defenses may exist where businesses have implemented reasonable practices for preventing unsolicited communications, but the application of such defenses often tends to be fact-specific.

B. **Mobile Texting**

Some laws specifically ban mobile marketing texting, including texts via short message service ("SMS") or other means. SMS marketing messages to cell phones may be actionable under the TCPA and also under the federal CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act). The TCPA, which has been construed as applying to text messages, allows recipients of illegal marketing spam to sue for damages measured based on actual monetary losses or $500 per violation, whichever is greater. FCC rules also prohibit unsolicited marketing text messages to a wireless number if they are sent using an autodialer, or if that number is on the national Do-Not-

Call list, though some have argued that the FCC rule does not apply to phone-to-phone texts. If, however, texts are sent from a computer to a phone, then the CAN-SPAM Act (rather than TCPA) applies to the text messages. There is no private right of action for individual consumers under the CAN-SPAM Act, but a company may face enforcement by regulatory agencies or Internet access service providers.

Federal law does not preempt state laws dealing with labeling or consent requirements for unsolicited e-mail where such laws govern misleading or deceptive communications. For instance, the California Business and Professions Code bans text message advertisements to cell phones or pagers. The law provides consumers a private right of action under existing state unfair business practices law to recoup the cost of each unwanted message received. Washington law is even more explicit as to text messages, and expressly prohibits unsolicited commercial electronic SMS messages to Washington residents. This has a broader reach than Washington's commercial email law, in that it applies to all messages and not solely those that are deemed misleading. Other states also provide for a private right of action, and some states allow such actions by Internet service providers against businesses that transmit unlawful emails through those providers.

Enforcement in these areas may increase. Phone carriers, for example, are increasingly cracking down on unlawful marketing texts by enabling customers to easily report SMS spam by forwarding the message to an established number.

C. **Call Recording and Monitoring**

Laws governing the recording and monitoring of phone calls with customers vary among the 50 states and federal government, and case law provides a broad interpretation of such laws in some instances. A minority of state laws have been interpreted to prohibit call recording by a party to the call where not all parties to the call consent. California law, for example, allows a private right of action to those injured by unlawful call recording and permits statutory damages of $5,000 per violation.

Unsolicited Commercial Email Marketing

Marketing email laws generally require (among other things) that a commercial email clearly identify the sender and subject matter, and provide the reader an opportunity to opt out of future messages from that sender. The federal CAN-SPAM Act prohibits the use of deceptive subject lines and false headers in unsolicited commercial emails, and requires senders to provide an opportunity to opt out of future messages. Where recipients exercise their right to opt out, businesses cannot thereafter send unsolicited commercial emails.

The FTC, FCC and state Attorneys General are among those who can enforce the CAN-Spam Act, as can Internet access services; there is no private right of action for individuals to file claims. The FTC, for example, has adopted rules restricting unwanted commercial emails sent to *computers*, whereas the FCC has banned such emails sent to *wireless devices*, including those sent to cell phones and pagers if the message uses an address that includes an Internet domain name. Customers receiving unwanted commercial messages on wireless devices may file complaints with the FCC, which can lead to agency enforcement actions. Because the FCC's ban does not include emails that a recipient has forwarded from her computer to her wireless device, there is some dispute as to the applicability of the FCC rules to email accessed via smart phones and tablet devices. However, businesses might nonetheless be subject to FCC enforcement of those violations under a broad interpretation of the ban. Moreover, the FTC's rules may prohibit such activity, and the FCC can enforce FTC restrictions under certain circumstances (such as where the sender is a communications company).

The CAN-SPAM Act supersedes state law that expressly regulates the use of email to send commercial messages, except to the extent that any such law prohibits falsity or deception in a commercial email message. As such, nearly every state also has a law regulating unsolicited email marketing. These laws include varying degrees of protection for consumers. Interestingly, some such laws have been struck down for not specifically regulating *commercial* email messages as opposed to all such messages; Virginia's Computer Crimes Act was overturned, for example, because it impacted transmission of *all* unsolicited bulk emails,

including those containing speech protected by the First Amendment, and not just commercial emails..

California law prohibits the sending of (or advertising within) unsolicited commercial emails containing misleading or falsified headers, and allows statutory penalties for any such email sent from California or to a California email address. The statute authorizes a private right of action, in which a recipient can recover actual damages and up to $1,000 per unlawful email, or up to $1 million per incident (as well as attorney's fees and costs). Importantly, the laws of California (and several other states) also enable an email service provider to sue those who send spam from its network or to its subscribers; such a provider can seek civil damages up to $25,000 per day, plus attorney's fees.

In 2010, the California Supreme Court found that a commercial email sender did not misrepresent its identity when it used random – but accurate and traceable – domain names so as to avoid spam filters. However, the Court's legislative parsing made clear that liability can be very fact-specific. In fact, in February 2012, the California Court of Appeal held that commercial email sent using a domain name that neither identifies nor is readily traceable to the actual sender constitutes misrepresentation in violation of California's law, and that the federal CAN-SPAM Act did not preempt this state statute. The case law is still developing and businesses should be cautious regarding marketing emails.

Some states have established affirmative requirements for commercial emailing, such as requiring "ADV" to appear in the subject line. While these types of provisions are generally preempted by CAN-SPAM in so far as they require labels on unsolicited commercial email, provisions merely addressing falsity and deception may remain in place.

Marketing Faxes

Under federal law, it is unlawful to send unsolicited advertisements to any fax machine, including those at both businesses and residences (with some exceptions for established business relationships). Generally, a business on whose behalf a fax is sent may be liable even if it did not physically send the fax. A third party may also be liable if it had a "high degree of

involvement" in the fax message — in which case it must also identify itself on the fax. Federal law also provides a private right of action against a party who sends unsolicited fax advertisements.

Registering a home phone number on the national Do-Not-Call list prevents only telephone solicitations, not fax advertisements to the home fax number. Nonetheless, consumers receiving unsolicited commercial faxes can file complaints with the FCC, and both the FCC and FTC can impose civil penalties of up to $11,000 per violation. State laws generally authorize consumers to file TCPA-related complaints with state authorities, or to bring private suits for actual monetary loss or statutory damages. Some states, such as Texas, criminalize the sending of unsolicited faxes during certain hours of the day. Under some laws, courts may treble damages for willful or knowing violations.

Gathering and Use of Consumer Information for Marketing Purposes

There have been a series of investigative articles regarding online marketing that have resulted in the filing of private lawsuits. The use by companies of "flash" cookies, for example, to assist in targeted marketing has resulted in the filing of a number of class action lawsuits alleging that consumers' choice was not honored. In general, companies should be cautious about the ways in which information is gathered and used, and the disclosures made about the use of consumer information.

In addition, some courts have given broad interpretation to laws governing this area. In early 2011, for example, the California Supreme Court issued an opinion in *Pineda v. Williams-Sonoma* holding that "personal identifiable information" under California Civil Code section 1747.08 includes a cardholder's zip code. Thus, the collection and recording of a zip code in connection with a credit card transaction may violate California law and may subject a business to claims for statutory penalties. A Massachusetts court also recently determined in *Tyler v. Michaels Stores* that zip codes are personal identification information under the state's consumer protection law. While the court found the Massachusetts law narrower in scope than California's law, it made clear that a company collecting zip codes may be found liable, particularly where a customer suffers identity theft.

Businesses that gather information for marketing purposes through electronic means may also be subject to claimed violations of computer crime statutes such as the Electronic Communications Privacy Act, the Stored Communications Act, the Computer Fraud and Abuse Act, and state equivalents. These laws may also provide for statutory penalties and attorneys' fees.

Some statutes relate to disclosure of uses by a business of consumer information. California's Shine the Light law requires businesses to disclose to inquiring consumers how information is shared for direct marketing purposes (or to allow consumers to opt out of such information sharing). Violations are punishable by civil penalties of $500 per violation, and $3000 for willful violations plus attorney's fees and costs.

Businesses that collect and use consumer information for marketing should assess their practices to determine whether action should be taken to mitigate against potential alleged violations of applicable laws, as these laws are sometimes broadly interpreted by plaintiffs, and in some instances, the courts.

Marketing to Children

The Children's Online Privacy Protection Act applies special rules to websites that collect personal information from children under the age of 13. The Act generally requires such a website to obtain parental consent before collecting, using, or disclosing a child's personal information. The website must also post notice of its information practices, specifying the type of information collected and how it is used and disclosed. The websites must give parents the right to review their children's personal information, as well as the right to request deletion or refuse to allow further collection or use of such information.

There are also state laws regulating marketing to children. For example, Michigan passed a law that applies to email marketing to children. Because Michigan law prohibits children from making certain purchases, the state allows parents and schools to register email addresses and other electronic contact points that children may access. Under the law, those who advertise or link to prohibited products and services must remove all registered contact points from their mailing lists.

Conclusion

State and federal privacy and marketing statutes create potential landmines for businesses to navigate when communicating with customers and potential customers. Because businesses are often unable to ascertain the geographic location of consumers receiving their communications, or are marketing nationally, businesses need to think broadly about the laws that might be applicable to their particular marketing practices.

Bio

Jim Snell is a partner in Bingham McCutchen's Silicon Valley office, where he represents clients in a broad range of complex commercial disputes, including patent litigation, trade secret and unfair competition claims, and false advertising and consumer class actions. He also regularly counsels and advises clients in ecommerce and privacy-related matters, including matters related to commercial email, security breaches, unsolicited facsimile laws, mobile and texting claims, computer crimes, and spyware. Mr. Snell is chair of Bingham's Privacy and Security Group and former co-chair of the firm's Intellectual Property Group. He is also a Certified Information Privacy Professional with the International Association of Privacy Professionals. He received his JD from the University of California, Hastings College of the Law. Mr. Snell can be reached at james.snell@bingham.com.

Courtney Smith is an associate in Bingham McCutchen's Silicon Valley office, where she advises clients on a broad range of litigation matters, including intellectual property, data privacy and security, and commercial litigation. She received her JD from Santa Clara University School of Law and her BA from Stanford University. Ms. Smith can be reached at courtney.smith@bingham.com.