# THE RISE OF PRIVACY LITIGATION — A SURVEY OF CAUSES OF ACTION AND CASES

By James Snell, Heather Shook and Monica Hernandez
Bingham McCutchen LLP

## A. OVERVIEW

The following is an outline of some privacy-related litigation issues. The outline starts with summary of some of the Federal and California claims made in privacy-related litigation. The outline then summarizes some of the cases addressing standing and injury in privacy-related litigation and also class action related issues in privacy-related litigation. The outline then summarizes some of the cases and developments relating to privacy-related claims (including apps and mobile issues; behavioral advertising, flash cookies and tracking cases; data breach cases; and unsolicited commercial email, facsimile and text cases). The outline is for informational purposes and does not constitute legal advice, and the cases cited should be referred to for an understanding of the holding. These summaries are not meant to be complete lists of relevant cases, but rather illustrative examples to give the reader an overview of some of the issues.

## B. PRIVACY RELATED CAUSES OF ACTION

### 1. Federal Law

#### 1.1. Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030)

The CFAA prohibits seven specific activities including: 1) obtaining national security information without authorization or in excess of authorized access from a computer; 2) obtaining information without authorization or in excess of authorized access from a financial institution computer, government computer, or protected computer; 3) intentionally accessing without authorization a government computer; 4) accessing a computer without authorization or in excess of authorized access with an

intent to defraud and obtain value; 5) causing damage while either transmitting a program or intentionally accessing a protected computer; 6) trafficking in passwords with an intent to defraud; and 7) extortion involving threats to damage a protected computer. In addition to prohibiting actual offenses, the CFAA also prohibits attempts to commit and conspiracy to commit offenses. **Private Right of Action:** Persons who suffer "damage or loss by reason of a violation of the CFAA" may recover compensatory damages, and injunctive or other equitable relief. The challenged conduct must cause either (i) a loss of at least $5,000 during a one-year period; (ii) physical injury; (iii) a threat to public safety; (iv) damage to a national security computer; or (v) damage to at least ten protected computers during a one-year period.

### 1.2. Electronic Communications Privacy Act (ECPA) (the Wiretap Act) (18 U.S.C. § 2510-2522)

The ECPA prohibits unauthorized individuals, and government agents acting without a warrant, from intentionally intercepting, using or disclosing any wire and electronic communication while in transit, including telephone or cell phone conversations, pagers, voicemail, email, and other computer transmissions. **Private Right of Action:** "[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" may bring a civil action to recover from the person or entity who engaged in the violation. For all actions except for private satellite video communication or certain radio communication, available relief includes equitable relief, damages, and reasonable attorneys' fees and costs. Damages are defined as either actual damages and profits, or whichever is greater between $100 per day for each violation or $10,000. Punitive damages are available.

### 1.3. Stored Communications Act (SCA) (18 U.S.C. §§ 2701-12)

The SCA prohibits (1) unlawful access to certain stored communications and (2) unauthorized disclosure of stored communications by electronic communication service and remote computing service providers. The SCA also limits the government's right to compel an electronic communications

service or remote computing service to disclose information in their possession about their customers and subscribers. **Private Right of Action:** Any "provider of an electronic communications service, subscriber, or other person aggrieved" may bring a civil action for violations, and is entitled to seek preliminary and equitable or declaratory relief, actual damages and any profits (and is entitled to no less than $1,000), and reasonable attorneys' fees and litigation costs. Punitive damages are available if the violation is willful or intentional.

### 1.4. Telephone Consumer Protection Act (TCPA) (47 U.S.C. § 227)

The TCPA governs telephone solicitations (i.e., telemarketing) and restricts the use of automatic dialing systems, artificial or prerecorded voice messages, SMS text messages received by cell phones, and the use of fax machines to send unsolicited advertisements. Unless the recipient has given prior express consent (or there is an established business relationship), the TCPA and the Federal Communications Commission (FCC) rules under the TCPA require solicitors to maintain a do not call list, to identify themselves and provide contact information, and to not call residences within specific hours (as well as other provisions). **Private Right of Action:** Allows for "actual monetary loss" or a $500 statutory penalty for each violation, whichever is greater, and treble statutory damages up to $1,500 where defendant "knowingly and willfully" violated the TCPA.

### 1.5. Controlling the Assault of Non-Solicited Pornography And Marketing Act ("The CAN-SPAM Act") (15 U.S.C. § 7701 et seq.)

The CAN-SPAM Act establishes rules for "commercial messages," including email and text messages (if the message uses an Internet address). The CAN-SPAM Act requires, among other things, that commercial messages contain an identification that they are unsolicited or an advertisement, a means to opt-out of future messages, a legitimate return physical address, and subject lines that are not false or misleading. Senders are also prohibited from using an automated means to harvest email addresses, or to

register multiple email accounts. The Act provides for civil and criminal penalties for noncompliance, including statutory damages up to $6 million for willful violations and, in some cases, prison terms of up to five years. **Private Right of Action:** There is no private right of action for recipients of commercial messages, but the CAN-SPAM Act does authorize the federal government, state attorneys general, and Internet Access Services to bring actions against violators.

### 1.6. Children's Online Privacy Protection Act (COPPA) and Children's Online Privacy Protection Rule (the Rule) (16 C.F.R. § 312)

This law applies to operators of commercial websites and online services directed to children under 13 that collect, use or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using or disclosing personal information from children under 13. The law generally prohibits website operators from knowingly collecting personally identifiable information from children under 13 without parental consent or without notice of their information practices. It also requires website operators to collect only personal information that is "reasonably necessary" for an online activity. **Private Right of Action:** State and federal agencies have authority to enforce the Act (though not the Rule), while the FTC can (and has) brought actions against website operators for violations of the Rule, which include civil penalties of up to $11,000 per violation.

### 1.7. Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681 et. seq.)

The FCRA regulates the disclosure of personal information held by consumer reporting agencies to third parties (but does not restrict the amount or type of information that can be collected). **Private Right of Action:** A consumer may recover actual damages and attorneys' fees for a negligent violation of the act, and for willful noncompliance, a minimum of $100 and a maximum of $1,000 plus punitive damages.

### 1.8. Video Privacy Protection Act (18 U.S.C. § 2710)

The law prohibits videotape service providers from disclosing customer rental records without the informed, written consent of the consumer. Furthermore, the law requires video service providers to destroy personally identifiable customer information within a year of the date it is no longer necessary for the purpose for which it was collected. The law contains several exceptions and limitations. **Private Right of Action:** Any "person aggrieved" may bring an action for actual damages but not less than liquidated damages in an amount of $2,500, punitive damages, and reasonable attorneys' fees and litigation costs.

## 2. California Law

### 2.1. California Constitutional Right to Privacy (Cal. CONST. art. 1, § 1)

The California Constitution grants each citizen an "inalienable right" to pursue and obtain "privacy," which the California Supreme Court has held is broader than rights recognized by the federal constitutional. **Private Right of Action:** The right of privacy may be enforced against private entities that seriously invade a protected privacy interest (where there is a reasonable expectation of privacy) and injured persons may collect damages resulting there from.

### 2.2. California's Unfair Competition Statute ("UCL") (Cal. Bus. & Prof. Code § 17200)

The UCL prohibits unfair competition, defined as any "unlawful, unfair, or fraudulent business act or practice." **Private Right of Action:** Any "person who has suffered injury-in-fact and has lost money or property" as a result of unfair competition may bring a civil action for injunctive relief and restitution.

### 2.3. California's Consumer Legal Remedies Act ("CLRA") (Cal. Civ. Code § 1750)

The CLRA prohibits "methods of competition and unfair or deceptive acts or practices undertaken by any person in a

transaction intended to result or which results in the sale or lease of goods or services to any consumer." **Private Right of Action:** "Any consumer who suffers any damage as a result of the use or employment by any person of a method, act, or practice declared to be unlawful" may recover actual damages (a class action requires a minimum of $1,000), restitution, punitive damages, attorneys' fees and costs.

### 2.4. California's "Shine the Light" Law (Cal. Civ. Code § 1798.3)

This law requires disclosure by any business that, in the prior calendar year, disclosed personal information about a customer to a third party and knows or reasonably should know that the third party used the information for direct marketing purposes. **Private Right of Action:** Violations are subject to civil penalties of $500 per violation ($3,000 per violation if willful) plus attorneys' fees and costs.

### 2.5. California's Transparency in Supply Chains Act (Cal. Civ. Code § 1714)

This law requires large retail sellers and manufacturing companies doing business in California to publicly disclose what, if any, efforts they have taken to eliminate slavery and human trafficking from their supply chains. The law does not require companies to take any remedial steps to combat slavery or human trafficking. Exclusive enforcement of the law is vested with the Attorney General. **Private Right of Action:** Although the law expressly does not create a private right of action, it does state that "[n]othing in this section shall limit remedies available for a violation of any other state or federal law." It also provides a right to injunctive relief.

### 2.6. California's Song-Beverly Act of 1971 (Cal. Civ. Code §§ 1747-1748.7)

This law prohibits, among other things, businesses from requesting cardholders to provide "personal identification information" during credit card transactions and then recording that information. **Private Right of Action:** The person paying with a credit card

may bring an action to recover a civil penalty not to exceed $250 for the first violation and $1,000 for each subsequent violation. The statute creates an exception if the violation results from a *bona fide* error made notwithstanding the defendant's maintenance of procedures reasonably adopted to avoid such an error. The California Supreme Court held in *Pineda v. Williams-Sonoma Stores, Inc*., 51 Cal. 4th 524 (2011) that ZIP code information is personal identification information under the act. (Similarly, in Massachusetts, General Law section 105(a) has been interpreted by *Tyler v. Michaels Stores, Inc*., 2012 WL 32208 (D. Mass. Jan. 6, 2012) to hold that a ZIP code is personal identification information.)

### 2.7. California's Unsolicited Commercial Email Law (Cal. Bus. & Prof. Code § 17529 et. seq., § 17538.45)

This law regulates unsolicited commercial email and requires a recipient to "opt-in" to receiving commercial email. Section 17529.5 concerns unsolicited commercial emails with misleading or falsified headers or information, and includes penalties. It applies to email sent to or from a California email address. **Private Right of Action:** This law authorizes the recipient, an email service provider or the Attorney General to bring an action for actual damages and liquidated damages of $1,000 per email advertisement sent in violation, up to $1 million per incident, as well as attorneys' fees and costs. The court shall reduce the liquidated damages to $100 per violation up to $100,000 in the event that it finds defendant implemented procedures and practices reasonably designed to prevent violations. Section 17538.45 gives an email service provider the right to sue those who send commercial email from its network or to its subscribers. Service providers can get civil damages up to $25,000 per day plus attorneys' fees.

### 2.8. California's Comprehensive Data Access and Fraud Act (Cal. Penal Code § 502)

This law prohibits computer crimes involving computer hacking, email spoofing, denial-of-service attacks, and introduction of

malware and other computer viruses into a computer or computer system. The prohibited acts under Section 502 generally track the prohibited acts under the CFAA. **Private Right of Action:** The owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation may bring a civil action for compensatory damages and injunctive relief or other equitable relief, punitive or exemplary damages for willful violations, and attorneys' fees.

### 2.9. California's Invasion of Privacy Act (Cal. Penal Code § 630 et. seq.)

This law prohibits the interception of, or eavesdropping upon and recording of, a confidential communication, under certain circumstances, without the knowledge or consent of all parties. **Private right of action:** Any person injured by a violation make bring an action for statutory damages of $5,000 or three times actual damages, whichever is greater, as well as for injunctive relief.

### 2.10. California's Online Privacy Protection Act of 2003 (OPPA) (Cal. Bus. & Prof. Code §§ 22575-22579)

The OPPA requires operators of commercial web sites or online services that collect and record personal information from California residents to post a privacy policy (and comply with its policy). The policy must detail the information gathered on the website and how the information is shared with other parties, as well as a process for the use to view and make changes to their information. **Private Right of Action:** This statute does not provide a private right of action, but it is possible claims could be filed under California's Unfair Competition Law.

### 2.11. California's Disposal of Consumer Records Law (Cal. Civ. Code §§ 1798.80-1798.81, 1798.84)

This law requires businesses to shred, erase, or otherwise modify the personal information when disposing of consumer records under their control. It provides a "safe harbor" from civil litigation for a business that has come into possession of records containing personal information that were abandoned, so long as the business

disposes of them as provided in the statute. **Private Right of Action:** Any consumer injured may recover damages, and any business that violates, proposes to violate, or has violated the statute may be enjoined.

### 2.12. California's Financial Information Privacy Act (CalFIPA) (Cal. Civ. Code §§ 4050-4060)

This law prohibits financial institutions from sharing or selling personally identifiable nonpublic information without obtaining a consumer's consent, as provided. It provides for a plain-language notice of the privacy rights it confers. The law requires that (1) a consumer must "opt in" before a financial institution may share personal information with an unaffiliated third party, (2) consumers be given an opportunity to "opt out" of sharing with a financial institution's financial marketing partners, and (3) consumers be given the opportunity to "opt out" of sharing with a financial institution's affiliates, with some exceptions. When an affiliate is wholly owned, in the same line of business, subject to the same functional regulator and operates under the same brand name, an institution may share its customers' personal information with the affiliate without providing an opt-out right. **Private Right of Action:** Though only the Attorney General or a state regulator can bring an action, an entity that negligently discloses or shares nonpublic personal information in violation is liable for a civil penalty not to exceed $2,500 per violation, and if there is more than one individual, damages are not to exceed $500,000.

### 2.13. California's Identification Devices, Prohibition on Bodily Implanting Law (Cal. Civ. Code § 52.7)

This law prohibits a person from requiring, coercing, or compelling any other individual to undergo the subcutaneous implanting of an identification device. The law specifically requires that it be liberally construed to protect privacy and bodily integrity. **Private Right of Action:** Provides for the assessment of civil penalties for violation, as specified, and allows an aggrieved party to bring an action for damages and injunctive relief.

### 2.14. California Insurance Information and Privacy Protection Act (Cal. Ins. Code §§ 791-791.28)

This law governs the collection, use and disclosure of personal information gathered in connection with insurance transactions by insurance companies, agents or insurance-support organizations. It generally prohibits disclosure of personal or privileged information collected or received in connection with an insurance transaction unless the disclosure is authorized in writing by the individual or is necessary for conducting business. The individual must be given an opportunity to opt-out of disclosure for marketing purposes. **Private Right of Action:** Any person whose rights are violated may apply for appropriate relief, and if their information is disclosed, monetary damages not to exceed actual damages sustained, plus costs and reasonable attorneys' fees.

### 2.15. California's Physical and Construction Invasions of Privacy Law (Cal. Civ. Code § 1708.8)

This law defines physical invasion of privacy in terms of trespassing in order to capture an image, sound recording or other impression in certain circumstances. It also defines constructive invasion of privacy as attempting to capture such an impression under circumstances in which the plaintiff had a reasonable expectation of privacy. **Private Right of Action:** Recovery of up to three times the amount of general and special damages proximately caused by a violation, punitive damages, and, if the violation was for a commercial purpose, disgorgement of any proceeds.

### 2.16. California Security Breach Information Act and related laws (Cal. Civ. Code §§ 17981.5, 1798.82, 1798.84)

This statute requires businesses that maintain unencrypted computerized data that includes personal information, as defined, to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is an individual's name plus one or more of the following: Social Security number, driver's license or

California Identification Card number, financial account numbers or password for accessing financial accounts, and medical or health insurance information. The notice must contain specific information, and any agency, person, or business that is required to issue a breach notice to more than 500 California residents must electronically submit a single sample copy to the Attorney General. The law also requires safeguards to ensure the security of Californians' personal information and to contractually require third parties to do the same. **Private Right of Action:** Any customer injured may bring a civil action to recover damages, and a civil penalty of $3,000 per violation for willful, intentional, or reckless violation, an injunction, and reasonable attorneys' fees and costs.

### 2.17. California's Anti-Phishing Act of 2005 (Cal. Bus. & Prof. Code §§ 22948-22948.3)

This act prohibits "phishing," the act of posing as a legitimate company or government agency in an email, web page, or other Internet communication in order to trick a recipient into revealing his or her personal information. **Private Right of Action:** A person who is engaged in providing Internet access service to the public, or owns a web page or trademark that is adversely affected by a violation may seek to recover the greater of actual damages or $500,000. An individual who is adversely affected may bring an action against a person who has directly violated the law the greater of actual damages or $5,000, and for injunctive relief.

### 2.18. California's Consumer Protection Against Computer Spyware Act (Cal. Bus. & Prof. Code §§ 22947-22947.6)

This act prohibits an unauthorized person from knowingly installing or providing software that performs certain functions, such as taking control of the computer or collecting personally identifiable information, on or to another user's computer located in California. The law also prohibits users from installing software by intentionally misrepresenting that the software protects the users privacy or security and is necessary in order to access content. **Private Right of Action:** This statute does not provide a

private right of action, though claims may be available under California's Unfair Competition Law.

### 2.19. California's Identity Theft Laws (Cal. Civ. Code § 1798.92-1798.97, Cal. Penal Code § 1202.4)

This law protects victims of identity theft who are sued for non-payment of debt created by identity thieves. **Private Right of Action:** Victims may bring an action against a claimant to establish they were the victim of identity theft, and to seek an injunction against the claimant, plus actual damages, costs, a civil penalty of $30,000 (if certain conditions are met), and other relief. Victims may also seek from the thief an award of restitution for expenses of monitoring the victim's credit report and for the costs to repair the credit.

### 2.20. California's Telemarketing, Do-Not-Call Law (Cal. Bus. & Prof. Code §§ 17590-17594)

This law governs telephone solicitations and maintains California's do-not-call registry, and provides an exemption for small businesses (which according to the FCC is preempted by the TCPA). **Private Right of Action:** Any person who has received a prohibited telephone solicitation may bring a small claims action for an injunction. After obtaining and serving notice of the injunction, any person who receives another unlawful telephone solicitation may be awarded a civil penalty of $1,000.

### 2.21. California's Telephone Number Directory (Cal. Pub. Util. Code § 2891.1)

This statute requires a subscriber's express permission before a cell phone service provider can list the subscriber's number in a directory. **Private Right of Action:** Every deliberate violation is grounds for a civil suit by the aggrieved subscriber against the organization or corporation and its employees responsible for the violation.

#### 2.22. California's False Advertising Law (Cal. Bus. & Prof. Code § 17500 et. seq.)

This law prohibits any company or individual from making false statements or statements likely to mislead consumers about the nature a product or service. **Private Right of Action:** Provides for restitution and injunctive relief, including on behalf of others if certain standing requirements are met.

#### 2.23. Common Law Invasion of Privacy

This law provides recovery for four distinct types of invasions: (1) public disclosure of embarrassing private facts; (2) publicity that places a person in a false light in the public eye; (3) physical intrusion on a person's solitude or seclusion, or into a person's private affairs; and (4) appropriation of a person's name or likeness, for defendant's advantage. **Private Right of Action:** Actual damages are recoverable if plaintiff can show a reasonable expectation of privacy and that defendant's conduct caused the damage.

## C. STANDING AND INJURY ISSUES

### 1. Federal Standing

#### 1.1. *First American Financial Corp. v. Edwards*, (argued Nov. 2011 before United States Supreme Court)

This case presents the question of whether a plaintiff can bring suit seeking a statutory damage award when she suffered no particular injury-in-fact. The case was argued in November 2011 and a written decision is pending.

#### 1.2. *Fraley v. Facebook, Inc.*, No. 11–CV–01726, 2011 WL 6303898 (N.D. Cal. Dec. 16, 2011)

Plaintiffs alleged that defendant's advertising practice of placing social media members' names, profile pictures, and an assertion that the members "liked" certain advertisers on other members' pages constituted unlawful misappropriation of the members'

names and likeness. Plaintiffs also alleged that defendant's commercial misappropriation was concrete and particularized with respect to each plaintiff, and plaintiffs' alleged injury was actual and traceable to defendant's action. The district court denied defendant's motion to dismiss for lack of Article III standing, finding that alleged violation of a statutory right (California's publicity rights statute) satisfied Article III's injury requirement. The court found that plaintiffs could argue that they were economically injured because their individual, personalized endorsements had concrete value, which could be measured by the additional profit defendant earned from the advertising technique compared to its sale of regular advertisements. The court also concluded that plaintiffs had standing to bring a UCL claim, finding they sufficiently established that they suffered an injury-in-fact and lost money as a result of defendant's alleged unfair action.

#### 1.3. *Del Vecchio v. Amazon.com, Inc.*, No. 11-C-00366 (W.D. Wash. Dec. 01, 2011)

Plaintiffs sued defendant for allegedly violating the CFAA and Washington's Consumer Protection Act (CPA), and for common law trespass to chattels and unjust enrichment. The district court dismissed plaintiffs' claims for failure to allege injury-in-fact. The court concluded that plaintiffs' allegations of economic losses resulting from defendant acquiring more user information than it was entitled to, and thus depriving plaintiffs of the opportunity to exchange their valuable information, were entirely speculative. Plaintiffs also failed to allege "a specific showing of injury" by alleging that defendant's transfer of cookies to their computers diminished their computers and constituted an interruption in service. The court also dismissed plaintiffs' CFAA and Washington's CPA claims because defendant had informed visitors it would place browser and Flash cookies on visitors' computers. Plaintiffs' trespass to chattels claim failed because plaintiffs did not shown that defendant's interference caused any plausible harm to their computers. Lastly, plaintiffs' unjust enrichment claim was dismissed for failure to allege that plaintiffs conferred any legally cognizable benefit upon defendant or that there would be anything inequitable about defendant's use of the information it collected.

### 1.4. *Low v. LinkedIn*, No. 11-CV-01468, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011)

Plaintiff alleged that defendant disclosed plaintiff's personal information, including browsing history, to third party advertising and marketing companies via cookies. The district court granted defendant's motion to dismiss, finding no injury-in-fact where plaintiff alleged he was embarrassed and humiliated by the disclosure of his personally identifiable browsing history, and that his browsing history had marketing value, which plaintiff lost as a result of defendant's conduct. The court noted that it was unclear whether the information was disclosed or transmitted to a third party, which might support a claim of emotional harm. The court further held that plaintiff's claims of economic harm were too abstract and hypothetical to satisfy an injury. Plaintiff had not alleged that his personal information was exposed to the public, or how transfer of information to a third party harmed him.

### 1.5. *In re iPhone/iPad App. Consumer Privacy Litigation*, 11-MD-02250 (N.D. Cal. Sep. 20, 2011)

Plaintiffs brought a class action alleging that defendant violated their privacy rights by allowing third party applications to make use of their personal information without their consent or knowledge. The court granted defendant's motion to dismiss finding no injury where plaintiffs failed to identify what personal information was accessed and what harm resulted. The court found no concrete harm alleged, and found that plaintiffs identified no particularized example of economic injury or harm to their computer, but instead alleged abstract concepts such as opportunity cost, value-for-value exchanges, consumer choice, and diminished performance. The court distinguished *Doe 1* (see below) on the basis that there were no specific allegations of danger of public disclosure of highly sensitive information. The court also distinguished the *Facebook Privacy Litigation* case (see below) which held that plaintiffs had alleged injury-in-fact on the basis that the Wiretap Act does not require an injury, but explicitly provides standing for a violation alone. The court also found that the alleged injuries were not fairly traceable to the defendants, and that there were no allegations that defendant misappropriated data.

### 1.6. *Bose v. Interclick, Inc.*, No. 10 Civ. 9183, 2011 WL 4343517 (S.D. N.Y. 2011)

Plaintiff brought a class action against defendants for allegedly violating the CFAA. The district court granted defendants' motion to dismiss plaintiff's CFAA claim on the basis that plaintiff failed to assert personal economic loss because plaintiff did not quantify any damage that defendants caused to her computer that could require economic remedy, such as repair cost or cost associated with investigating the alleged damage. Plaintiff failed to allege specific damage due to the alleged interruption of service, such as slowdown or a shutdown of her computer. Further, the court held that defendants' collection of plaintiff's personal information does not constitute damage or loss. Finally, the court held that even if the putative class was allowed to aggregate their damages, the representative plaintiff must still demonstrate that she herself has been personally injured.

### 1.7. *Cohen v. Facebook, Inc.*, 798 F.Supp.2d 1090 (N.D. Cal. June 28, 2011)

Plaintiffs alleged that defendant misappropriated their names and likeness to promote its "Friend Finder" service. The district court granted defendant's motion to dismiss plaintiffs' claims for misappropriation and violation of the Lanham Act. The court found that plaintiffs failed to allege injury because their names and likeness were only displayed on the Facebook pages of people who were already their friends. Thus, plaintiffs could not show any harm, noting that the names and likeness were not publicized in any way that they were not already published. The court also rejected the argument that the availability of statutory damages could, by itself, satisfy injury, and found that "[p]laintiffs must, at a minimum, plead that they suffered mental anguish from the misappropriation, and a plausible factual basis for any such assertion."

### 1.8. *La Court v. Specific Media, Inc.*, No. SACV-10-1256, 2011 WL 2473399 (C.D. Cal. Apr. 28, 2011)

The district court dismissed plaintiffs' claims for lack of Article III standing. The court dismissed the claims on the grounds that

plaintiffs failed to adequately allege an "injury-in-fact" because plaintiffs did not specifically allege that defendant actually tracked the online activities of any named plaintiff. The court concluded that unauthorized collection of personal information by itself does not result in injury without something more. The court also found that plaintiffs failed to show that a single individual was deprived of any economic value resulting from defendant's alleged conduct of taking their personal information. Further, the court found that plaintiffs' argument that they had suffered harm to their computers because Flash cookies diminish the computers' performance was a de minimis allegation of harm not rising to the level of Article III standing.

### 1.9. *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010)

Plaintiffs brought a class action for negligence and breach of contract where a laptop allegedly containing sensitive unencrypted employee data was stolen. The district court held that plaintiffs' allegations that theft of defendant's laptop subjected them to increased risk of future identity theft was sufficient to establish injury-in-fact for purposes of Article III standing. However, the court granted defendant's motion to dismiss for failure to allege cognizable injury under state law. The Ninth Circuit affirmed, holding that plaintiffs alleged a credible threat of real and immediate harm stemming from the theft of defendant's laptop that contained their unencrypted personal information. If the laptop had not been stolen, the risk of future identify theft would be less credible. Accordingly, the court held that plaintiffs whose personal information was stolen but not misused have suffered an injury sufficient to confer standing.

### 1.10. *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102 (N.D. Cal. 2010)

Plaintiffs brought a nationwide class action alleging that defendant violated the ECPA and California's UCL and FAL. The district court found that plaintiffs had Article III standing to seek injunctive relief, and had stated claims under the CLRA, UCL, and FAL. Plaintiffs alleged that after defendant publicly disclosed

plaintiffs' confidential Internet search records and sensitive personal information, defendant continued to engage in the practice of storing search queries containing confidential information, and did not take steps to ensure that such information would not be disclosed again. The court found these facts to be sufficient to allege an ongoing injury for purposes of demonstrating standing to seek injunctive relief. The court found that plaintiffs had sufficiently pled injury for purpose of stating a claim under the CLRA because the collection and disclosure of plaintiffs' sensitive information was not something plaintiffs bargained for when they signed up and paid fees for defendant's service. The court found that plaintiffs had sufficiently stated a claim under the UCL and FAL based on allegations that defendant misled plaintiffs by assuring them through its privacy policy that its service was "safe, secure and private."

### 1.11. *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)

Plaintiffs, environmental groups, challenged regulations issued pursuant to the Endangered Species Act of 1973 (ESA) regarding the geographic area to which it applies. The Supreme Court held that plaintiffs lacked standing to bring a claim under the ESA. The Court ruled that in order to establish standing plaintiffs must show that they suffered an actual or imminent injury-in-fact that is concrete and particularized. The Court held that plaintiffs did not assert sufficiently imminent injury to have standing and plaintiffs' alleged injury was not redressable. First, the Court found that plaintiffs failed to show that one or more of their members would be directly affected apart from their special interest in the subject. Plaintiffs' allegations that they intended to revisit project sites at some indefinite future time, at which time they would presumably be denied the opportunity to observe endangered animals, were not sufficient to establish standing because they do not demonstrate an "imminent" injury. Second, the Court held that redress of the only injury-in-fact plaintiffs complain of requires action by the individual governmental funding agencies, and any ruling the Court might make against the Secretary was not likely to produce that action as the ruling would not be binding upon the agencies.

## 2. Injury Under California Law

### 2.1. *Kwikset Corp. v. Superior Court,* 51 Cal. 4th 310 (Cal. 2011)

Plaintiff alleged that defendant violated California's UCL by selling locks with a "Made in U.S.A." label where the locks allegedly contained some foreign-made components. The district court overruled the defendant's demurrer. The Court of Appeal reversed, directing the trial court to sustain the demurrer and dismiss the action, and holding that even if plaintiff's "patriotic desire to buy fully American-made products was frustrated,' that injury was insufficient to satisfy the standing requirements of [California Business and Professions Code] sections 17204 and 17535." The California Supreme Court reversed. The Court held that injury-in-fact has a "well-settled meaning" under federal law and is "an invasion of a legally protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical." The Court also held that lost money or property, or economic injury, is itself a classic form of injury-in-fact and "[i]f a party has alleged or proven a personal, individualized loss of money or property in any nontrivial amount, he or she has also alleged or proven injury in fact." The Court then held that a plaintiff who relied on a label when making a purchase will have suffered economic harm by having "paid more for [a product] than he or she otherwise might have been willing to pay if the product had been labeled accurately."

### 2.2. *Hall v. Time Inc.*, 158 Cal. App. 4th 847 (Cal. Ct. App. 2008)

Plaintiff alleged that defendant violated California's UCL by sending an invoice for a book before the end of the free trial period, allegedly to induce the customer to send payment. Plaintiff further alleged that the fraudulent conduct caused plaintiff to believe he did not have a two-week trial period. The court held that plaintiff did not allege he suffered an injury-in-fact because although he expended money, he received the book in return and therefore did not suffer an injury or harm. The court also held that plaintiff did not allege injury causing any actual and compensable

damage because plaintiff "did not allege he lost money or property as a result of [defendant's] unlawful practice."

## D. CLASS ACTIONS

### 1. Federal Actions

#### 1.1. *Mazza v. American Honda Motor Co., Inc.,* 666 F.3d 581 (9th Cir. 2012)

Plaintiffs filed a nationwide class action against defendant under California law. The Ninth Circuit vacated the nationwide class certification on the grounds that there were no predominating common issues of law as California's consumer protection statutes may not be applied to a nationwide class with members in 44 jurisdictions. These jurisdictions have materially different consumer protection laws and remedies available than California. The court held that variances in state law overwhelm common issues and preclude predominance for a single nationwide class. Each class member's consumer protection claim should be governed by the laws of the jurisdiction in which the transaction took place. Additionally, the court held that no common questions of fact predominate because individual determinations are required as to whether class members were exposed to misleading advertisements and whether they relied on those advertisements.

#### 1.2. *O'Shea v. Epson America, Inc.,* No. 09–CV-8063, 2011 WL 4352458 (C.D. Cal. Sept. 19, 2011)

Plaintiff alleged that defendant violated California's UCL and FAL by failing to disclose and affirmatively misrepresenting material information. The district court denied plaintiff's motion for nationwide class certification under Rule 23(b)(3), finding plaintiff failed to satisfy the predominance requirement. Additionally, unnamed class members, like the class representative, must also satisfy Article III's standing requirements, but because many class members purchased defendant's printer from websites that did not publish the alleged misrepresentations, individualized issues of injury and causation permeated the class claims.

### 1.3. *Wal-Mart Stores, Inc. v. Dukes,* 131 S.Ct. 2541 (2011)

Plaintiffs brought a class action alleging that defendant violated Title VII of the Civil Rights Act of 1964 by discriminating against women. The district court certified the class, and the Ninth Circuit affirmed. The Supreme Court reversed. The Court held that the class did not have common questions of law or fact under Rule 23(a) because there was no corporate wide policy of discrimination that applied to all workers, but rather the discrimination claims were based on hundreds of thousands store level employees and supervisors. The Court rejected plaintiffs' allegations that defendant's policy of allowing local supervisors to have discretion over employment matters established a basis of liability because it did not find that all of defendant's supervisors exercised their discretion in a common way with some common direction. The Court also held that plaintiffs' back pay claims were improperly certified under Rule 23(b)(2) because this rule only applies when a single, indivisible remedy can provide relief to each class member, and claims for monetary relief that are not incidental to the requested injunctive or declaratory relief do not qualify.

### 1.4. *AT&T Mobility LLC v. Concepcion,* 131 S.Ct. 1740 (2011)

Plaintiffs brought a putative class action alleging that defendant engaged in false advertising and fraud. The cell phone contract between plaintiffs and defendant provided for arbitration of all disputes, but did not permit class-wide arbitration. The district court denied defendant's motion to compel individual arbitration and the Ninth Circuit affirmed. The Supreme Court reversed, holding that the Federal Arbitration Act ("FAA") preempts California's judicial rule regarding the unconscionability of class arbitration waivers in consumer contracts. California's Supreme Court had previously ruled in *Discovery v. Superior Court*, 36 Cal. 4th 148 (2005) that a contract could not bar class-wide arbitration if the contract is an adhesion contract, the dispute involves small amounts of damages, and the consumers allege a scheme to defraud. The Court held that the *Discovery Bank* rule is preempted by the FAA because requiring class-wide arbitration would

interfere with fundamental attributes of arbitration and make the process slower, more costly, and more likely to cause procedural morass than final judgment.

### 1.5. *Faherty v. CVS Pharmacy, Inc.*, No. 09-CV-12102, 2011 WL 810178 (D. Mass. May 9, 2011)

Plaintiff, a Massachusetts resident, filed a motion to certify a nationwide class action or, alternatively, a statewide class. The district court denied plaintiff's motion for nationwide class certification, but provisionally allowed the motion to certify a statewide class of Massachusetts residents. The court explained that to certify a nationwide class, it would have to apply a state-by-state legal analysis for the class members who resided in the 43 states (plus the District of Columbia) in which defendant did business. The court concluded that the intricate nature of the analysis and the potential for juror confusion militated against the certification of a nationwide class. Additionally, because consumer protection laws vary considerably between states, the court could not apply one state's law.

### 1.6. *Webb v. Carter's Inc.*, 272 F.R.D. 489 (C.D. Cal. 2011)

Plaintiffs brought a putative class action alleging that defendants breached implied warranties and violated California law. The district court denied plaintiffs' motion for class certification, finding that unnamed class members, like the named plaintiffs, must satisfy Article III standing in a federal court class action. The court found that plaintiffs failed to show that the proposed class members suffered an injury-in-fact to establish standing because the overwhelming majority of children who wore defendant's garments suffered no adverse effects and the levels of chemicals in the clothes did not exceed standards established by law. The court further found that plaintiffs failed to establish that common questions predominate. The court noted that where material misrepresentations are made, an inference of reliance is raised as to the entire class. However, in this case, individual issues predominated because consumers would differ in what they considered material and whether they would still buy the garments

if they saw defendant's disclosure. Further, the actual reliance and harm elements were not susceptible to class-wide proof. Lastly, the court concluded that a class action is not the superior method because defendant was already offering the relief that plaintiffs seek (refunds for the garments and up to $250 for medical expenses).

### 1.7. *Avritt v. Reliastar Life Ins. Co.*, 615 F.3d 1023 (8th Cir. 2010)

Plaintiffs brought a putative class action alleging that defendant engaged in unfair business practices. The district court denied plaintiff's motion for class certification, and the Eight Circuit affirmed, holding that class certification was not appropriate under Rule 23(b)(3) because plaintiffs' claims involve a number of individual issues that could not be resolved on a class-wide basis. The court reasoned there were two or more reasonable interpretations of the contract, and therefore, extrinsic evidence about what each party intended when it entered the contract would be required. Extrinsic evidence would also be necessary to determine defendant's intent, how the contract was explained in various sales discussions, whether each member's understanding of the contract was consistent with the theory that the named plaintiff advanced, and what each member's expectations were. Because each class member's experiences vary, the court held that defendant's liability to the entire class cannot be established with common evidence. Lastly, the court held that plaintiffs' focus on monetary damages, and not on injunctive or declaratory relief, precluded Rule 23(b)(2) certification.

### 1.8. *Vinole v. Countrywide Home Loans, Inc.*, 571 F.3d 935 (9th Cir. 2009)

Plaintiffs filed a putative class action alleging that defendant violated the Fair Labor Standards Act and state law. Defendant filed a motion to deny certification before plaintiffs filed a motion for certification and prior to the pretrial motion deadline and discovery cutoff. The district court granted defendant's motion, and the Ninth Circuit affirmed, holding that Rule 23 does not preclude a defendant from bringing a preemptive motion to deny

class certification. The Court explained that there was no procedural prejudice from the timing of the motion because plaintiffs had ample time to prepare and present their certification argument, and could have requested an extension or continuance after defendant filed its motion. Further, the court held that denial of plaintiffs' class certification was proper because individual issues predominated over common issues, explaining that an individualized analysis of how each class member spent their time would be required to determine whether that member was an "exempt" employee.

### 1.9. *Murray v. Financial Visions, Inc.*, No. 07-CV-2578, 2008 WL 4850328 (D. Ariz. 2008)

Plaintiffs brought a class action against defendants alleging that every email intercepted by defendants constituted a violation of the ECPA and violated their privacy rights under state law. The district court denied plaintiffs' class certification motion under Rule 23(b), holding that certification would be improper under Rule 23(b)(2) because the predominant remedy sought was monetary damages, and under Rule 23(b)(3) because defendant's liability under the Wiretap Act would require an individualized showing of each class member's knowledge and consent. Plaintiffs' invasion of privacy claim and issue of damages also would require individual hearings to determine whether each class member had a reasonable expectation of privacy and to quantify each class members' emotional injuries. While the court did not decide the typicality requirement, it noted that it is generally lacking when the representative plaintiff's claim is against a defendant unrelated to the defendant against whom the class claims are brought. However, this limitation does not apply where all injuries are the result of a conspiracy between the defendants. The court also did not decide the adequacy of the representative plaintiffs, but noted that a representative's loyalty to the class will be questioned when he files a separate claim against one of the defendants in the class action.

#### 1.10. *Chambers v. Time Warner,* No. 00-CIV-2839, 2003 WL 749422 (S.D. N.Y. 2003)

Plaintiffs alleged that defendants violated copyright law and the Lanham Act by exploiting their recordings. The district court dismissed plaintiffs' amended complaint, and the Court of Appeals vacated and remanded. On remand, the district court denied plaintiffs' motion for class certification, finding that plaintiffs failed to establish adequacy of representation under Rule 23(a). Because the class representatives' claims and the defendant against whom those claims were made had been dismissed, the class representatives had little knowledge of the remaining defendant and were not familiar with the misconduct involved in the class action, and therefore the court found that they would be unable or unwilling to protect the interests of the class.

### 2. State Actions

#### 2.1. *Knapp v. AT&T Wireless Services, Inc.,* 195 Cal. App. 4th 932 (Cal. Ct. App. 2011)

Plaintiff brought a class action alleging that defendant violated California law and acted fraudulently. Plaintiff alleged that defendant's description of its wireless service plans were misleading because defendant's billing practice was to round up any partially used minute for a call to the next full minute. The district court denied plaintiff's motion for class certification, and the Court of Appeal affirmed on the ground that common issues of fact did not predominate. The court held that defendant did not make uniform representations to the proposed class members and, as a result, an individual inquiry would be required to determine whether the representations received by each class member constituted misrepresentations, omissions, or nondisclosures.

#### 2.2. *Sevidal v. Target Corp.,* 189 Cal. App. 4th 905 (Cal. Ct. App. 2010)

Plaintiff brought a class action alleging that defendant violated California law by making misrepresentations. The district court denied plaintiff's motion for class certification, and the Court of Appeal affirmed. The court held that plaintiff failed to meet the

class certification requirements that there be an ascertainable class and that common questions of law and fact predominate over the class. The court made a factual finding that class members were not ascertainable because defendant did not maintain, or have access to, records identifying the individuals who purchased a product with an erroneous country-of-origin designation. The Court also held that the proposed class was overbroad because a substantial portion of the class was not exposed to the alleged misrepresentation.

### 2.3. *In re Tobacco II Cases*, 46 Cal. 4th 298 (Cal. 2009)

Plaintiffs alleged that defendants violated California's UCL by conducting deceptive advertising campaigns. The district court certified the class, but later granted defendant's motion to decertify the class based on Proposition 64's amendment to the UCL. Proposition 64 requires a showing of injury-in-fact and loss of money or property as a result of the alleged unfair competition. The Court of Appeal affirmed, but the California Supreme Court reversed to the extent that the decertification was based on the requirement that all class members need to demonstrate Proposition 64 standing. The court held that the standing requirements are applicable only to the class representative and not to unnamed class members. Moreover, a class representative is not required to prove individualized reliance on specific misrepresentations when the unfair practice is part of an extensive and long-term advertising campaign.

### 2.4. *Kaufman v. ACS Systems, Inc.*, 110 Cal. App. 4th 886 (Cal. Ct. App. 2003)

Plaintiffs brought a class action alleging that defendant sent them unsolicited facsimile advertisements in violation of the TCPA. The district court granted plaintiffs' motion for class certification. The Court of Appeal affirmed, holding that the TCPA does not foreclose class actions, but not every TCPA action should proceed as a class action. Though there was concern that unfairness would result to the defendants if a class were certified, plaintiffs argued, and the court agreed, that the fairness of the statutory penalty for a violation of the TCPA had been decided by Congress in enacting

the law, therefore the court should not consider whether a class action would be unfair to the defendant when deciding whether a class action is the superior method of adjudication. Conversely, the court noted that class certification has been denied on the grounds that a common question did not predominate where a defendant allegedly violated the TCPA through a series of individual transmissions under individual circumstances. The court noted that certification has also been denied where the court would be required to conduct individual inquiries with regard to each potential class member. For the reasons stated above, the court concluded that the decision of whether to certify a class should be decided on a case-by-case basis. In deciding this issue, courts should consider whether there is an ascertainable class and a well-defined community of interest among the purported class members.

## E. APPS AND MOBILE ISSUE DEVELOPMENTS

### 1. FTC Staff Report Regarding Mobile Apps

The FTC issued a staff report titled *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing* on February 16, 2012, discussing the results of a survey of mobile applications for children. The FTC enforces the Children's Online Privacy Protection Act (COPPA) and the FTC's COPPA Rule, which require operators of online services, including mobile apps, to provide notice and get parental consent before collecting information from children under 13. The report raises privacy questions about apps and opines that app developers and app stores in many cases do not advise parents on what data is being collected from their children, the purpose for such collection, how it is gathered, how it is being shared, who collects it, or who will have access to it. The FTC also stated that app stores that provided information about the data collection and sharing practices of apps may only offer the general "permission" statements and fail to offer the information mentioned above. Mobile apps can automatically gather and share personal information, such as the user's precise geolocation, phone number, contact lists, call logs, unique identifiers, and other information stored on the device. The report found that app stores may leave the bulk of disclosure to

individual app developers and the FTC instead recommended that app stores, as gatekeepers of the app marketplace, provide a designated space for developers to disclose information and provide standardized icons to signal features. The FTC also recommended that data practices information be provided in simple and short disclosures, apps disclose whether the app connects with social media, apps disclose whether the app contains targeted ads, and that third parties that collect data disclose their privacy practices. The FTC stated that it will conduct an additional review in the next six months to determine whether mobile apps are violating COPPA and whether enforcement is appropriate.

### 2. California AG Statement of Principles

On Feb. 22, 2012, California Attorney General Kamala D. Harris released a "Joint Statement of Principles" with smart phone industry leaders to clarify privacy protections for users of mobile applications ("apps"). According to the Attorney General, the Principles are designed to improve compliance with California's Online Privacy Protection Act, which requires operators of commercial websites and other online services that collect personal user data to post detailed privacy policies. The Joint Principles set forth a series of best practices. For example, smart phone companies should make app privacy policies available to consumers before the point of downloading. The Principles also state that companies should implement processes to allow consumers to report apps that do not comply with applicable terms of service and/or laws. The Attorney General plans to revisit these issues in the next six months, and has warned that app developers who do not comply with their stated privacy policies will face prosecution under California's Unfair Competition Law and False Advertising Law.

### 3. Carrier IQ Litigation (70+ lawsuits filed around the country)

Carrier IQ provides data and analytics software tools for smart phones to mobile network operators and device manufacturers. The software is designed to provide operators and manufacturers with comprehensive diagnostic metrics on the performance of smart

phone devices used on the operators' networks. However, starting in November 2011, Trevor Eckhart, a security researcher, posted a series of videos analyzing Carrier IQ's software (IQ Agent) on his smart phone and claiming that the software was a hidden "rootkit" that logs a device user's information (including keystrokes, text messages, web searches, and secure URL (HTTPS) connections) and sends it to Carrier IQ, network operators, and/or device manufacturers. As a result of these allegations, more than 70 law suits (mostly class actions) were filed across the country against Carrier IQ and various mobile network operators and device manufacturers. The plaintiffs have generally asserted claims under the Wiretap Act and various state unfair competition and privacy laws.

## F. BEHAVIORAL ADVERTISING, FLASH COOKIES, AND TRACKING CASES

### 1. *In the Matter of Scanscout Inc.*, No. 102-3185, 2011 WL 5591677 (F.T.C. Nov. 8, 2011)

The FTC alleged that defendant violated the FTCA by misleading users on how to opt out of receiving cookies. Defendant gave its users instructions on how to opt out of receiving cookies by changing their browser settings, but defendant allegedly used Flash cookies which are not controlled through a computer's browser. The FTC alleged that defendant's opt out guidelines were false and misleading as users could not prevent defendant from collecting data about their online activities by changing their browser settings. The FTC entered a consent order with the defendant to not misrepresent the extent of its user data collection or the extent to which users may exercise control over the collection, use, and disclosure of data collected from their online activities. The order also required defendant to place a clear notice on its website stating that it collects user Internet activities, and to provide an opt-out link.

**2. *In the Matter of Chitika, Inc.*, 151 F.T.C. 494, 2011 WL 3568985, FTC File No. 102 3087, Decision and Order (Dkt. No. C-4324, dated June 7, 2011)**

The FTC alleged that defendant violated the provision of the FTCA through its business of online behavioral advertising. Defendant allegedly made false and misleading statements in its privacy policy that consumers could opt out of targeted advertising for a reasonable period; however, the opt out expired after 10 days. The FTC entered a consent order with the defendant to not misrepresent the extent of its data collection about consumers and the extent to which consumers may exercise control over the collection, use, and disclosure of data collected from their online activities. Further, the order requires defendant to make the opt out option easier for consumers to execute and extends the life of the opt out to a minimum of five years.

**3. *In re Facebook Privacy Litigation*, 791 F.Supp.2d 705 (N.D. Cal. 2011)**

Plaintiffs alleged that defendant intentionally transmitted personal information about them to third-party advertisers without their consent, in violation of the ECPA and state laws. The district court dismissed plaintiffs' claims. The court found that plaintiffs failed to state an ECPA claim because the information disclosed by defendant was sent to either defendant or advertisers, which are addressees or intended recipients. The court found that plaintiffs failed to state a CFAA claim because defendant did not act "without permission," as there were no technical barriers blocking defendant from accessing its own website. The court also found that plaintiffs failed to allege they suffered an injury-in-fact because personal information does not constitute property for purposes of California's UCL.

**4. *Mortensen v. Bresnan Communications LLC*, No. 10–CV-00013, 2010 WL 5140454 (D. Mont. Dec. 13, 2010)**

Plaintiffs sued defendant for allegedly installing cookies on their personal computers and transmitting their electronic activities to third parties. The district court dismissed claims under the ECPA finding plaintiffs consented to the terms of use and did not have an

objectively reasonable expectation because defendant had provided notice. The court also declined to dismiss the CFAA claims, finding that while only economic losses over $5,000 are recoverable, plaintiffs could aggregate their damages; the court also found that the cookies "exceeded authorization" under the CFAA. The court further declined to dismiss plaintiffs' trespass to chattel claim finding defendant's intentional and unauthorized interference with plaintiffs' computer systems could proximately result in damage.

#### 5. *Keithly v. Intelius Inc.*, 764 F.Supp.2d 1257 (W.D. Wash. 2011)

Plaintiffs brought a class action alleging that marketing techniques used by defendant to promote a third party's services were deceptive. The district court dismissed the SCA claim, finding defendant was not an electronic communication service provider. The court further found that the marketing technique by which acceptance of a discount unknowingly enroll consumers in a third party's services could be deceptive, the marketing technique which informed consumers that acceptance of a discount would enrolled them in a third party's services was not deceptive, and the marketing technique by which the decision to take a survey in exchange for a discount resulted in transfer of the consumers' account information and enrollment in a third party's service could be deceptive.

### G. DATA BREACH CASES

#### 1. *Whitaker v. Health Net of California*, No. 11-S-0910 (E.D. Cal. Jan. 19, 2012)

A third party that managed defendant's information technology infrastructure, informed defendant that it lost nine server drivers (six of which had subsequently been recovered) containing private information of approximately 800,000 of defendant's customers. Defendant sent a letter to affected customers, and a lawsuit followed. Defendant moved to dismiss for lack of injury, which the court granted, finding plaintiffs did not allege any actual harm, apart from the loss of the data and the risk that the data may be misused.

### 2. *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011)

Plaintiffs alleged that the unauthorized use of credit and debit card data after hackers breached defendant's electronic payment processing system breached a fiduciary duty owed and an implied contract, was negligent, and violated the Maine Unfair Trade Practices Act (UTPA). The district court dismissed the claims finding lack of injury and that plaintiffs failed to state a breach of fiduciary duty claim. The First Circuit affirmed the dismissal of the fiduciary duty claim, holding there was no allegations of a confidential relationship or that defendant abused a position of trust. The court also affirmed dismissal of the UTPA claim, holding plaintiffs improperly alleged the same damages resulting from the acts that formed the basis of their negligence and implied contract claims. The court reversed dismissal of the implied contract claim, finding a factual issue as to whether there was an implied contract that defendant would not use the credit card data for improper means and would take reasonable measure to protect the information. The court also reversed dismissal of the negligence claim, finding plaintiffs could seek to recover actual financial losses from credit and debit card misuse, including reasonable mitigation damages (though not time spent monitoring credit).

### 3. *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3rd Cir. 2011)

An unknown hacker allegedly gained access to plaintiffs' personal and financial information maintained by defendant. The district court dismissed plaintiffs' claims of negligence and breach of contract for lack of standing and failure to state a claim. The Third Circuit affirmed, holding that the plaintiff did not adequately allege damage, injury, and ascertainable loss based on allegations of an increased risk of identity theft, need to incur costs to monitor their credit activity, or emotional distress. The court found no evidence that the data had been or would be misused, and therefore any injury was too speculative or hypothetical.

#### 4. *Claridge v. RockYou, Inc.*, 785 F.Supp.2d 855 (N.D. Cal. 2011)

Plaintiff alleged defendants failed to secure and safeguard plaintiff's sensitive personally identifiable information (PII). The court dismissed plaintiff's claims for violation of California's UCL, California's CCL, California's CLRA, and breach of the implied covenant of good faith and fair dealing. The court found that loss of PII was not loss of money or property, as required for a UCL claim. The court also found that a CCL claim does not require defendant to provide a sufficiently secure computer system, or subject to liability individuals or entities who took no active role in tampering with, or in gaining unauthorized access to computer systems, and therefore defendant could not be liable under the CCL. Further, plaintiff had no claim under the CLRA because he was not a "consumer." The court declined to dismiss plaintiff's claims for breach of contract, breach of implied contract, and negligence *per se*. The court found that plaintiff had sufficiently alleged a general basis for harm for his contractual and negligent based claims by alleging that the breach of his PII had caused him to lose some ascertainable "value" and/or property right inherent in the PII.

#### 5. *Ruiz v. Gap, Inc.*, 380 Fed. Appx. 689 (9th Cir. 2010)

Plaintiff sought damages and injunctive relief based on the alleged theft of a laptop computer that contained his social security number. The district court held that plaintiff had standing to pursue his claims, but granted summary judgment in favor of defendant. The Ninth Circuit affirmed, holding that plaintiff failed to establish sufficient non-speculative, present harm to support a cause of action for negligence and breach of contract under California law. Plaintiff's unfair competition claim failed because standing is limited to individuals who suffer actual losses of money or property, and thus are eligible for restitution. Plaintiff's invasion of privacy claim failed because courts have not extended the concept of an "egregious breach" to include an increased risk of privacy invasion. Lastly, plaintiff's claim under California Civil Code section 1798.85 failed because requesting social security

information from applicants after the password-protected website was accessed does not violate the statute.

#### 6. *Amburgy v. Express Scripts, Inc.*, 671 F.Supp.2d 1046 (E.D. Mo. 2009)

The district court dismissed plaintiff's complaint in its entirety for lack of standing, finding his alleged injuries of an increased risk of identity theft, time spent monitoring credit accounts, loss and compromise of personal information, and loss of exclusive control over such information, are not compensable.

### H. UNSOLICITED COMMERCIAL EMAIL CASES

#### 1. *Facebook, Inc. v. Power Ventures, Inc.*, No. 08-C-05780 (N.D. Cal. Feb. 16, 2012)

Plaintiff alleged that Defendant allowed its website users to access their Facebook account through their website, and induced its users to send emails to other Facebook users regarding the website. Plaintiff has an authorized developer program, which defendant did not participate in, and plaintiff undertook some measures to prevent access to defendant and its website users. The district court granted summary judgment against defendant, dismissing claims under the CAN-SPAM Act, California Penal Code section 502, and the CFAA. The Court held that inducing users to send messages to their Facebook friends (by offering them $100) constitutes "initiat[ing]" a message, that the emails were misleading because the header information did not say defendant's website name, and therefore defendant violated the CAN-SPAM act. The Court further held that circumventing a technical barrier, which defendant did because they used software designed to evade IP address blocks, established a right to relief under California Penal Code section 502. Finally, the court granted summary judgment on the CFAA claim, similarly finding that the access was "without authorization," and that plaintiff satisfied the $5,000 damage threshold.

**2. *Hafke v. Rossdale Group*, LLC, No. 1:11-CV-220, 2011 WL 4758768 (W.D. Mich. Oct. 7, 2011)**

Plaintiff filed a claim under Michigan's "Unsolicited Commercial E–Mail Protection Act" with the county court in Michigan. Defendant removed the complaint to the district court, and the court denied plaintiff's motion to remand on the grounds that the court has federal question jurisdiction under the CAN-SPAM Act. The court then dismissed the action because the CAN-SPAM Act expressly preempts any state statute that regulates the use of email for commercial messages unless the statute prohibits "falsity or deception." The court held the alleged technical violations relating to header, sender, and opt-out information preempted under the CAN-SPAM Act as they were not materially deceptive actions.

**3. *Cicero v. American Satellite, Inc.*, 2011 Ohio 4918, 2011 WL 4477247 (Ohio Ct. App. Sept. 27, 2011)**

Plaintiff alleged that defendant violated the Ohio Consumer Sales Practices Act by sending him allegedly deceptive email advertisements that failed to include applicable terms and conditions as required. The district court granted defendant's motion for summary judgment, and the Court of Appeals affirmed. Because plaintiff conceded he was not at any time deceived by the email advertisements because he was aware of the advertisement's hidden terms and conditions, the court held that plaintiff was not entitled to recover.

**4. *Facebook, Inc. v. MaxBounty, Inc.*, No. 10-CV-4712 (N.D. Cal. Mar. 28, 2011)**

Plaintiff alleged that defendant created fake Facebook pages that were intended to re-direct unsuspecting Facebook users away from Facebook.com to third party commercial websites. Plaintiff brought claims under the CAN-SPAM Act, the Computer Fraud and Abuse Act, fraud, tortious interference with contract, breach of contract, federal trademark dilution, and false designation of origin. Defendant moved to dismiss the CAN-SPAM Act claim on the ground that the communications were not "electronic mail messages" under the Act. The Court rejected defendant's argument and found that the CAN-SPAM Act applies to commercial

electronic communications directed through routing activity to specific destinations. Therefore, the court found, commercial messages on or in Facebook walls, news feeds, message inboxes, and user profiles fall within the scope of the CAN-SPAM Act and its regulations. Defendant also argued that plaintiff failed to state a claim under the CFAA because it did not specifically plead an intent to defraud as required under Federal Rule of Civil Procedure 9(b). The Court found that intent to defraud is not the same as fraud, and therefore plaintiff did not need to plead intent to defraud with greater specificity.

**5. *Martin v. CCH, Inc.*, 784 F. Supp. 2d 1000 (N.D. Ill. 2011)**

Plaintiff alleged that defendant violated the Illinois Electronic Mail Act (IEMA) by sending him an unsolicited advertising email. The district court granted defendant's motion to dismiss, finding that the IEMA requirement of an "ADV" label at the beginning of the subject line of an email was expressly preempted by the CAN-SPAM Act. The court found that the CAN-SPAM Act preempts any state statute or regulation that controls the use of email for commercial messages, unless the statute or regulation specifically prohibit "falsity or deception" in commercial e-mails. The court also found that the CAN-SPAM Act does not provide standing for an individual private citizen to file a private cause of action.

**6. *Hypertouch, Inc. v. ValueClick, Inc.*, 192 Cal. App. 4th 805 (Cal. Ct. App. 2011)**

Plaintiff alleged defendants violated California's CEL by sending commercial emails that contained deceptive "header information." The district court granted defendant's summary judgment motion, and the Court of Appeal reversed. The court held California's CEL is not preempted because the CAN-SPAM Act's savings clause applies to state law that prohibits material falsity or material deception in a commercial email regardless of whether such laws require the plaintiff to establish all of the elements of common law fraud. The court explained that California's CEL and the CAN–SPAM Act provide that defendants can be liable for deceptive subject lines and header information without regard to plaintiff's

knowledge or mental state, and regardless of whether anyone was actually deceived. Thus, the court found that plaintiff need not establish that defendants sent the offending emails or that defendants had knowledge of such emails. The court also concluded that the content of email is misleading, "[i]f a subject line creates the impression that the content of the email will allow the recipient to obtain a free gift by doing one act (such as opening the email or participating in a single survey), and the content of the email reveal that the 'gift' can only be obtained by undertaking more onerous tasks … the subject line is misleading about the contents of the email."

### 7. *Ferron v. Echostar Satellite LLC,* 410 Fed. Appx. 903 (6th Cir. 2010)

Plaintiff alleged that defendants sent him email advertisements in violation of the Ohio Consumer Sales Practices Act (OCSPA). The district court granted defendant's motion for summary judgment, and the Sixth Circuit affirmed, holding that plaintiff solicited, received, and saved defendants' email advertisements in order to bring the lawsuit. Accordingly, the court ruled that individuals who solicit emails from an advertiser, after having researched and discovered the terms of the advertisement, cannot prevail under the OCSPA (i.e., individual plaintiffs cannot take the role of private attorney generals).

### 8. *Kleffman v. Vonage Holdings Corp.,* 49 Cal. 4th 334 (Cal. 2010)

Plaintiff brought a class action alleging that defendant sent unsolicited email advertisements from multiple domain names for the purpose of bypassing spam filters in violation of California's CEL. The district court granted defendant's motion to dismiss for failure to state a claim. The Court of Appeals certified a question of law, asking the California Supreme Court to decide whether sending unsolicited commercial email advertisements from multiple domain names for the purpose of bypassing spam filters constitutes falsified, misrepresented, or forged header information under California's CEL. The California Supreme Court held that such conduct did not violate the CEL because an email with an

accurate and traceable domain name makes no affirmative representation or statement of fact that is false. The Court also noted that the claim was preempted by the CAN-SPAM Act.

**9. *Hoang v. Reunion.com*, No. 08-C-3518, 2010 WL 1340535 (N.D. Cal. Mar. 31, 2010)**

After reviewing the Ninth Circuit's reasoning in *Gordon* (see below), the district court reconsidered its 2008 order granting defendant's motion to dismiss plaintiffs' California's CEL claim, and reversed its ruling. The court found plaintiffs' allegation that they received commercial emails containing "false and deceptive" statements sufficient to establish standing to bring a claim under state law. Further, the court held that to allege standing, a plaintiff need not allege reliance and actual damage where the emails are arguably misleading.

**10. *Asis Internet Services v. Vistaprint USA, Inc*., 617 F. Supp. 2d 989 (N.D. Cal. 2009)**

Plaintiffs claimed that defendant violated California's CEL by allegedly sending unsolicited commercial emails that contained false advertisements. The district court denied defendant's motion to dismiss, finding that the phrase "falsity or deception" is not confined to strict common law fraud, and, as such, the court found that plaintiffs' claim was not preempted by the CAN-SPAM Act.

**11. *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040 (9th Cir. 2009)**

Plaintiff alleged that defendant violated the CAN–SPAM Act and Washington law. The district court granted defendant's motion for summary judgment, and the Court of Appeal affirmed. The court held that a threshold issue in private (ISP) actions alleging CAN-SPAM Act violations is whether plaintiff has standing including whether (1) plaintiff is an Internet access service provider and (2) whether the plaintiff was adversely affected by statutory violations. On the first issue, plaintiff was not an Internet access service provider because he played no more than a nominal role in providing Internet-related services and made minimal efforts to block spam messages. Nor was plaintiff adversely affected by

spam because he was not a *bona fide* Internet access provider, and he did not experience harm beyond the mere annoyance of spam and greater than the negligible burdens typically borne by an IAS provider. Moreover, the court held the state law violations were preempted based on the reasoning of *Mummagraphics* (see below).

### 12. *MySpace v. Wallace*, 498 F. Supp. 2d 1293 (C.D. Cal. 2007)

Plaintiff filed a motion for a preliminary injunction alleging defendant was violating the CAN-SPAM Act and California's CEL. The district court granted in part plaintiff's motion, enjoining defendant from "hijacking" MySpace.com users' profiles to disseminate commercial messages and solicitations to other MySpace.com users. The court found that sending messages, comments, and bulletins to MySpace.com users, as alleged, fell within the CAN-SPAM Act's definition of commercial email messages. The court also found that the Act not only prohibits sending messages with inaccurate header information, but also sending messages with accurate header information, access to which was obtained through false or fraudulent pretenses. Further, the court noted that it was likely that the alleged messages violated the CAN-SPAM Act as they were probably unsolicited and did not provide a functioning return electronic mail address to which recipient could respond to opt-out.

### 13. *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348 (4th Cir. 2006)

Plaintiffs alleged that defendant violated the CAN-SPAM Act and Oklahoma law. The district court granted defendant's motion for summary judgment, and the Eight Circuit affirmed, holding that the CAN-SPAM Act preempts Oklahoma law to the extent a claim is based on immaterial errors in email. Plaintiff's CAN-SPAM Act claims failed because the claimed inaccuracies did not amount to materially false or materially misleading information. The court granted summary judgment on plaintiff's trespass to chattels claim because plaintiff offered no more than nominal damages.

### 14. *Riddle v. Celebrity Cruises, Inc.*, 105 P.3d 970 (Utah Ct. App. 2004)

Plaintiffs alleged that defendant's Internet pop-up ads violated Utah's Unsolicited Commercial and Sexually Explicit Email Act. The district court granted defendant's motion for summary judgment, and the Court of Appeals affirmed. The court held that the alleged "pop-up" advertisements were not sent to specifically predefined destinations and they appeared on a computer user's screen only when the host website was called up by a user. Accordingly, even if a pop-up could be considered an email, it would be regarded as a solicited email and fall outside the scope of the Act. The court also held that "pop-up" advertisements do not fall within the ambit of Utah's Act and are not subject to the same limitations that the Act places on traditional email.

## I. UNSOLICITED FACSIMILE CASES

### 1. *Holtzman v. Turza*, No. 08-C-2014, 2010 WL 4177150 (N.D. Ill. Oct. 19, 2010)

Plaintiff brought a putative class action against defendant for allegedly violating the TCPA by sending class members one or more unsolicited advertisements by fax. The district court granted plaintiff's motion for summary judgment. Defendant argued that the editorial, non-advertising content of each fax made the advertising content "incidental" to the rest of the document. The court found that in considering each fax in its entirety and defendant's commercial purpose, the faxes constituted an unsolicited advertisement within the meaning of the TCPA. The court held defendant liable for all of the faxes received by members of the defined class, resulting in $4,215,000 in statutory damages ($500 for 8,430 faxes).

### 2. *CE Design, Ltd. v. Prism Business Media, Inc.*, 606 F.3d 443 (7th Cir. 2010)

Plaintiff, a design company, filed a claim against defendant for allegedly violating the TCPA. Plaintiff alleged that defendant sent it a single unsolicited fax advertisement without plaintiff's prior express consent. The district court granted defendant's motion for

summary judgment on the ground that it shared an "established business relationship" (EBR) with plaintiff based on plaintiff's status as a subscriber to defendant's publications. The Court of Appeal affirmed. In 2005, Congress passed the Junk Fax Protection Act (JFPA), which exempted from the TCPA any faxes sent "from a sender with an established business relationship with the recipient." However, the JFPA did not apply in this case because defendant sent the fax prior to the Act. The court looked to the FCC reports and orders implementing the TCPA and concluded that the EBR exemption applies pre-JFPA. The court also gave deference to the FCC's interpretation that the EBR defense applies to both individuals and businesses.

#### 3. *Missouri ex rel. Nixon v. American Blast Fax, Inc.*, 323 F.3d 649 (8th Cir. 2003)

The State of Missouri brought an action against defendant, alleging that defendant violated the TCPA by sending unsolicited advertisements via facsimile transmissions. The federal government intervened. The district court dismissed the action, finding that section 227(b)(1)(C) violated the First Amendment's guarantee of freedom of speech by making it unlawful to send an unsolicited advertisement to a fax machine. The Eight Circuit reversed, holding that the government demonstrated a substantial interest in preventing advertising cost shifting and interference with fax machines that unwanted advertising places on the recipients, the TCPA provision was reasonably related to the government's substantial interest, and the provision was not more restrictive or extensive than necessary to accomplish the government's substantial interest. Accordingly, section 227(b)(1)(C) satisfies the constitutional test for regulation of commercial speech.

### J. UNSOLICITED TEXT MESSAGES CASES

#### 1. *Ryabyshchuk v. Citibank (South Dakota) N.A.*, No. 11–CV–1236, 2011 WL 5976239 (S.D. Cal. Nov. 28, 2011)

Plaintiff alleged that defendant violated the TCPA by sending text messages to his cell phone without his consent. Defendant relied on plaintiff's initial complaint to argue that plaintiff "consented"

by providing his cell phone number to defendant when he applied for a credit card. Plaintiff later amended his complaint to remove any implication that he provided his number. The court ruled that plaintiff was allowed to revise his pleadings, and based on the pleadings it was unclear whether plaintiff released his number "knowingly." Moreover, the court ruled that the burden of showing consent lies on the sender of the alleged unsolicited text message.

**2. *Gutierrez v. Barclays Group*, No. 10-CV-1012, 2011 WL 579238 (S.D. Cal. Feb. 9, 2011)**

Husband and wife plaintiffs allege that defendant negligently and willfully violated the TCPA. The district court denied defendant's motion to dismiss. The court concluded that the husband gave prior express consent to the use of his cellular number and to his wife's cellular number because he possessed "common authority" over the numbers. Nonetheless, the court found that plaintiffs revoked their consent (husband via responsive text message and wife orally) to defendant's use of their cellular numbers. Since prior express consent was revoked, defendant could not relay on the "prior express consent" exception. The court also found that the TCPA is intended to protect the telephone subscriber, and as such, the wife had standing. Further, the court found that TCPA does not require plaintiffs to show that they were charged for the calls or text messages to prevail on their claims.

**3. *Kramer v. Autobytel, Inc.*, 759 F. Supp. 2d 1165 (N.D. Cal. 2010)**

Plaintiff brought a putative class action against defendants (an advertiser and its client) under the TCPA for allegedly sending advertising text messages. The district court denied defendants' motion to dismiss, noting that the FCC and Ninth Circuit have explicitly stated that a text message is a "call" for the purpose of the TCPA, that both advertisers and advertisement broadcasters are liable under the TCPA, and that plaintiff's consent to receive promotional materials from one entity does not constitute consent to receive marketing from non-affiliated entities. The court found that in this early stage of the litigation, plaintiff does not have to

plead with particularity the size of the putative class or the content and date of the text messages he allegedly received.

#### 4. *Lozano v. Twentieth Century Fox Film Corp.*, 702 F. Supp. 2d 999 (N.D. Ill. 2010)

Plaintiff brought a putative class action alleging that defendant violated the TCPA by sending plaintiff advertising text messages without consent. The district court denied defendant's motion to dismiss, finding that plaintiff had sufficiently alleged a "call" because text messages are "calls" for purposes of the TCPA. The court noted that the plain language of the TCPA does not require plaintiff to allege that he was charged for the alleged text messages in order to state a claim. Moreover, the court concluded that plaintiff sufficiently alleged defendant's use of a random or sequential number generator by alleging that defendant's equipment *has the capacity* to store or produce telephone numbers. Further, the court found that this interpretation of section 227 was not an unconstitutional restraint on free speech because the TCPA directly advances a legitimate government interest of minimizing the invasion of privacy caused by unsolicited telephone communications to consumers, and the act is sufficiently tailored by only prohibiting the use of equipment with the capacity to randomly dial numbers.

#### 5. *Czech v. Wall Street on Demand, Inc.*, 674 F.Supp.2d 1102 (D. Minn. 2009)

Plaintiff brought a putative class action against defendant for sending unwanted text messages, asserting claims for violation of the CFAA and state law. The district court granted defendant's motion to dismiss plaintiff's federal CFAA claims, but denied the motion to dismiss plaintiff's state law claims. Plaintiff's claim that defendant obtained unauthorized information from her cell phone failed because she did not prove that defendant obtained any data. Plaintiff's claim that defendant intentionally caused damage to her cell phone failed because consuming limited resources, such as slowing the wireless device, depleting its memory, and interrupting service does not constitute damage. Plaintiff also failed to allege intentional conduct. Finally, the court noted that plaintiff's

allegations failed to plead facts supporting a conclusion that the "loss" that she incurred was a result of defendant's violations of the CFAA and she did not allege that she incurred charges due to her receipt of the unwanted text messages, or state the amount of those charges.

### 6. *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946 (9th Cir. 2009)

Plaintiff alleged that defendant violated the TCPA by sending plaintiff an advertising text message on her cellular telephone. The district court granted defendant's summary judgment. The Ninth Circuit reversed, holding that there was a genuine issue of material fact concerning whether the text message was sent by an automatic telephone dialing system (ATDS) prohibited under TCPA. In evaluating the issue of whether equipment is an ATDS, the court explained that a system need not actually store, produce, or call randomly or sequentially generated telephone numbers, it need only have the capacity to do it. The court also held that text messages are "calls" within the meaning of the TCPA and plaintiff did not consent to receiving the alleged text message by consenting to receive promotional material from the free ringtone provider (and its affiliates and brands). Since defendant was not an affiliate or brand of the free ringtone provider, plaintiff did not consent to receive text messages from defendant.

Authors

**James G. Snell**
Partner
Bingham McCutchen LLP
james.snell@bingham.com

Jim Snell is co-chair of Bingham's Privacy and Security Group and former co-chair of the firm's Intellectual Property Group. Jim represents clients in a broad range of complex commercial matters, including patent litigation, Internet and privacy issues, trade secret matters, matters involving unfair competition claims under California Business and Professions Code section 17200, false

advertising, and class actions. He has particular experience in privacy, Internet and marketing issues, including junk email laws, spyware issues, matters involving the Telephone Consumer Protection Act, and data security issues. He defended the first lawsuit filed under the CAN-SPAM Act as well as the first lawsuit filed under Michigan's Child Protection Registry. Jim has also handled cases involving novel issues of Internet law relating to the Communications Decency Act.

**Heather L. Shook**
Associate
Bingham McCutchen LLP
heather.shook@bingham.com

Heather Shook is a complex commercial litigator, whose practice focuses on privacy and data security, computer crimes, intellectual property, antitrust and commercial litigation. Prior to joining the firm, she worked for a defense team at the International Criminal Tribunal for the Former Yugoslavia in the Hague, Netherlands. Heather also served as a extern for the Hon. John Noonan at the United States Court of Appeals, Ninth Circuit.

**Monica A. Hernandez**
Associate
Bingham McCutchen LLP
monica.hernandez@bingham.com

Monica Hernandez advises clients on general litigation matters, including privacy matters.

Disclaimer

The above outline is for informational purposes and does not constitute legal advice.