Santa Clara Computer and High Technology Law Journal
April, 2009

Article

***883** POISED ON THE PRECIPICE: A CRITICAL EXAMINATION OF PRIVACY LITIGATION

Andrew B. **Serwin** [FNd1]

Abstract

The ever-increasing use of information, coupled with changes in computing technology that make information easier to use, and more portable, ensure that privacy litigation will be a focus of government enforcement and plaintiffs in years to come. This article examines trends in privacy litigation, common theories of liability, damage issues faced by plaintiffs, as well as an examination of class action ***884** issues as plaintiffs typically frame their allegations in the class action context.

I. Introduction

A collection of factors has caused the United States to be poised on the precipice of a new wave of litigation-litigation arising from the improper use or collection of information. Public concern over privacy is ever increasing while, and some would say because, information has become critical to our everyday existence. In what is now a self-reinforcing cycle, increased public concern has caused an exponential increase in regulations, and the new regulations have caused increased attention and public concern because many of the new laws require public disclosure of security breaches, which increases societal concerns over privacy.

Security breach laws, the laws that mandate public disclosure of data incidents, provide the best example of the increase in regulation. Just a few short years ago, California passed the first security breach law. Now, 43 other states, the City of New York, Washington, D.C., and Puerto Rico, have adopted laws and many other countries have either adopted, or are likely to adopt, security breach laws as well. Laws restricting the collection and use of social security numbers provide another example as more than 35 states have adopted these types of laws.

Whether the increasing public concern over privacy is caused by, or reflected in, the new privacy laws, the phenomenal expansion in the number of privacy laws will have a predictable effect-a geometric increase in the number of privacy laws will result in an equally geometric increase in the number of violations of privacy laws. As violations increase, there is an equally predictable consequence-increased incentives for individuals to attempt to enforce these new rights.

One of the first challenges in privacy litigation is to define what “privacy” litigation actually is. While consumer-based privacy litigation gains much of the attention, to focus exclusively on consumer-oriented privacy

litigation misses half the picture. The increase in value of information has increased the number of businesses that are bringing litigation to protect their intellectual capital and their networks. Though these claims are not thought of as "privacy" litigation in the traditional sense, these claims are no less about the improper use of information than actions brought by individuals. This litigation is frequently brought under the Computer ***885** Fraud and Abuse Act, the Electronic Communications Privacy Act, CAN-SPAM, and unfair competition law, including portions of the Lanham Act.

In the privacy realm, the Federal Trade Commission (FTC) serves as the primary federal privacy enforcer. However, the FTC does not have unlimited resources, privacy is not its only responsibility, and the actual number of enforcement actions is not as high as one might guess. As a result, state attorney generals have an important role to play in privacy enforcement. However, with limited exceptions, state attorney generals have not brought a significant number of privacy matters. As a result, enforcement in many cases falls to private plaintiffs, and they play a role in enforcing privacy laws where violations are alleged to have occurred.

However, the road to plaintiffs' recovery in privacy litigation is littered with a number of issues that can derail a case before it truly starts, not the least of which is that plaintiffs in many cases cannot prove actual damage, and may actually lack standing to bring an action. Moreover, even if the case clears this hurdle, many class actions fail the certification requirements because of issues unique to privacy litigation.

This article examines the common theories of privacy litigation, the issues faced by plaintiffs, and examines class action issues generally, as well as some class issues that are unique to privacy litigation. While privacy cases have had mixed success, the increased importance of information, coupled with increased public attention, and the ever-increasing number of privacy laws guarantees that we will be stepping off of the precipice and into privacy litigation.

II. An Overview of Privacy Litigation

While the volume of privacy litigation has recently grown, and the theories underlying cases have changed, privacy litigation has a long history at common law. Many prior privacy cases were predominantly founded upon common law theories and the Restatement of Torts. Now, while common law still plays a role, many theories of privacy litigation rely upon statutory violations. This article first examines the history of privacy litigation under common law, and then the common statutory theories are examined, as are other theories that are not exclusively statutory. The issues private plaintiffs face in bringing privacy litigation are examined, as are class certification issues, and finally privacy issues arising from class action discovery are also examined.

***886** III. Privacy Litigation at Common Law

The Restatement (Second) view of tort liability for privacy violations is generally consistent with state common law. [FN1] Specifically, the Restatement recognizes four distinct areas of liability: intrusion upon seclusion; appropriation of name or likeness; publicity given to private life; and publicity placing person in false light. [FN2]

The Restatement formulation of an intrusion upon seclusion finds liability where a person intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, if the intrusion would be highly offensive to a reasonable person. [FN3] It should be noted that liability does not de-

pend upon any publicity given to the person whose interest is invaded. This claim consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man. [FN4]

Liability for invasion of privacy based on appropriation of name or likeness exists when a person appropriates to his own use or benefit the name or likeness of another. [FN5] This typically arises when a person inappropriately uses a person's name or takes a photograph of a person and uses it in an inappropriate way without consent. The Restatement notes that the interest protected here is interest of the individual in the exclusive use of his own identity, as it is represented by his name or likeness, to the extent that the use may be of benefit to him or to others. [FN6]

Liability under the Restatement formulation can arise for publicity given to private life if one gives publicity to a matter concerning the private life of another, if the matter publicized is of a kind that would be highly offensive to a reasonable person, and is not of legitimate concern to the public. [FN7] The Restatement notes that this principal may not be consistent with the free speech rights afforded to ***887** individuals under the federal Constitution, as well as the rights of a free press. [FN8]

Finally, the Restatement imposes liability for publicity placing a person in false light. The elements of this tort are met if a person gives publicity to a matter concerning another that places the other before the public in a false light, if the false light in which the other was placed would be highly offensive to a reasonable person, and the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed. [FN9]

While the Restatement formulations are not binding in each state, most states follow these elements in some form and have also established common law liability that generally tracks these four categories, [FN10] so the Restatement is an important starting point to understanding common law privacy claims.

IV. Privacy Litigation-A Modern View

Modern privacy litigation is no longer exclusively reliant upon common law and the Restatement theories. Instead, it also relies upon myriad statutes that provide private rights of action. The most common are the Computer Fraud and Abuse Act (CFAA), [FN11] as well as the Electronic Communications Privacy Act (ECPA), [FN12] and CAN-SPAM, [FN13] though other theories are also utilized.

A. The CFAA

The CFAA was an anti-hacking law that has grown well beyond its original role. Now, it can serve as the basis of litigation by creative plaintiffs' class action attorneys, as well as companies attempting to protect their trade secrets. The law provides both civil and criminal remedies. [FN14]

Under the CFAA, it is a criminal act for anyone to intentionally access a computer without authorization, or beyond the scope of any ***888** authority that has been granted, whether the computer is owned by the government or not, if the conduct involved an interstate or foreign communication. [FN15] It is also a criminal act to knowingly, and with the intent to defraud, access a protected computer: (i) without authorization; or (ii) beyond the scope of any authorization, if the person furthers a fraud and an item of any value is obtained, if the value obtained is over $5,000 in any one year period. [FN16] Furthermore, it is unlawful for a person to knowingly

cause the transmission of a program, code, or command that intentionally: (1) damages a protected computer; (2) accesses a protected computer and recklessly causes damage; or (3) accesses a protected computer without authorization and causes resulting damage. [FN17]

1. Damage under the CFAA

The type of damage shown to establish a violation of this portion of the CFAA must be one of the following types: aggregated damage that exceeds $5,000; potential modification or impairment of a medical diagnosis, examination, treatment or care of one or more persons; physical injury; a threat to public health or safety; or damage to a government computer that is used in furtherance of the administration of justice, national defense, or national security. [FN18] There is no requirement that the damaged party have an ownership interest in the computers which were accessed. In one case, the Ninth Circuit rejected the defendant's argument that there must be a showing that the accessed computer belonged to the plaintiff. [FN19] Instead, it need only be shown that there was an act that violated the CFAA and that the plaintiff suffered damage-e.g., damage that results from the unauthorized access of data that is owned by the plaintiff, but stored on another's computer. [FN20]

The Ninth Circuit has also held that any “natural and foreseeable” expenses are part of the damages amounts that can be considered. [FN21] This includes impairments to the system, loss or ***889** recreation of data, or creating a more secure network. [FN22] However, numerous courts have held that economic damages, and not emotional distress or punitive damages, are recoverable. [FN23] The Northern District of California recently addressed whether forensic costs related to identifying an anonymous user who misappropriated information constituted “loss,” ultimately concluding that such costs were indeed a “loss.” [FN24]

In determining whether the requisite level of damage exists, a court can consider the hourly wage of any employees who repair any damage, even if the employees performed the repairs in the scope of their normal duties and were not paid any additional amounts. [FN25] While lost revenue, security checks, and other similar expenditures will not count towards the damage requirement if there is no showing that there was an actual compromise of the network, data, or programs on the network. [FN26] Other courts, however, have held that lost wages and payment of consulting costs would count towards the damage requirement, even if there is no physical damage. [FN27] Furthermore, other costs may count towards the $5,000 requirement. Attorneys' fees for bringing an action under the CFAA, however, do not count towards the loss requirement. [FN28]

A case from the district court in the Northern District of Indiana provides a good example of the issues faced by a plaintiff in a CFAA claim. [FN29] This court considered the damage element for a § 1030(a)(5) ***890** claim in the context of alleged misconduct by an attorney as she departed her former employer. [FN30] In Spangler, the defendant was a partner in a law firm and was alleged to have taken proprietary information, including client lists, and e-data files, before her departure from the firm as part of her plan to set up a competing law firm. [FN31] The plaintiff moved for summary judgment on its CFAA claim. [FN32] The court ultimately denied the request, noting that while the plaintiff had alleged that it incurred costs to investigate the alleged improper access, it did not show that there was any impairment of data or the system that supported a finding of losses qualifying as damage under § 1030(a)(5). [FN33]

The loss requirement under the CFAA for a civil action continues to befuddle courts. Indeed, two federal courts issued opinions on the issue within two days of each other, and reached opposite conclusions even though they relied upon the same cases to reach their conclusion. In P.C. of Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore, L.L.C., 2007 WL 708978 (D.N.J. 2007), some former employees allegedly took trade

secret and confidential information regarding the plaintiffs' business and used it to open up competing businesses. [FN34] The defendants brought a motion to dismiss the CFAA claim, asserting that the plaintiffs failed to state a claim under the CFAA, including because they had not demonstrated any "loss" under § 1030(a)(5)(B)(1), as required by § 1030(g). [FN35] The P.C. Yonkers court examined the Nexans Wires case, as well as the Resdev case, and concluded that these cases made a distinction between costs incurred as a result of an incident versus lost revenue or other consequential damages. [FN36] The court noted that loss is ***891** defined by the CFAA as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." [FN37] The court made a distinction when it concluded that the "interruption of service" requirement applied only to the portion of the definition that addresses "any revenue lost, cost incurred, or other consequential damages," but not to any allegation that related to "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." [FN38] Thus, the court read the definition of loss to have two different components-one of which does not require an interruption of service, if the loss relates to the costs of responding to an offense conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense; and a second component that includes lost revenue, incurred costs, or other consequential damages that result from an interruption of service. [FN39] Under this definition, the court concluded that the plaintiffs had stated a claim under the CFAA. Notably, plaintiffs in this matter never alleged there was either damage or an interruption of service, but rather that they had suffered "substantial losses in excess of $5,000, including but not limited to losses sustained in responding to defendants' actions, investigating defendants' actions and taking remedial steps to prevent defendants' further actions." [FN40] Nowhere did plaintiff articulate how it had suffered damage to a computer or an interruption of service.

Courts in the Ninth Circuit, however, continue to liberally permit claims under the CFAA where there is no clear allegation of system interruption, and therefore loss, as other courts have held. [FN41] Other ***892** courts, however, continue to reject this line of cases. [FN42] Either way, a number of issues await plaintiffs who seek to recover under the CFAA, though these issues are not insurmountable.

2. Examples of CFAA violations

a. Unauthorized Access to websites

The First Circuit upheld the granting of an injunction under the CFAA against a defendant that had used a "scraper" program to obtain confidential information from the plaintiff's website. [FN43] The information included pricing information that was obtained and used to undercut the plaintiff's prices. [FN44] The defendant had hired a former executive from the plaintiff who had allegedly used knowledge of the plaintiff's confidential information to assist in the development of the "scraper" program in violation of a confidentiality agreement. [FN45]

b. Gathering of E-mail Addresses

In a case that predated the enactment of CAN-SPAM, a Virginia District Court held that the defendants' harvesting of e-mail addresses from other AOL customers violated the CFAA, because the sending of large numbers of unsolicited commercial e-mails damaged AOL. [FN46]

***893** c. Diversion of Customers/Harvesting of Customer Lists

Diversion of customers can constitute a violation of the CFAA. In one case, a former programmer for a dating service allegedly used his knowledge of his former employer's software, as well as access codes, to route customers from the dating service to an adult oriented website. [FN47] The court concluded that these allegations, if true, constituted a violation of the CFAA. [FN48]

The improper gathering of customer lists can also constitute a violation of the CFAA. One court has held that the use of "bots" to obtain customer lists from the WHOIS database violated the CFAA. [FN49] In a related example, a district court recently applied Verio, at the pleading stage, finding on the allegations made in the case, that the use of a spider could potentially bind a company to an online agreement. [FN50]

The use of "bots" to gather information, including pricing information, in violation of the terms of use of a website can also violate the CFAA. For example, a court found sufficient allegations to support a claim for violation of the CFAA, where a company created a software program that allowed customers to search for airline fares online, and the data was obtained through the use of "bots," in violation of a user agreement. [FN51]

d. Defective Software

In certain cases, courts have held that defective software, in particular microcode, that causes damage to data on computers can constitute a "transmission" of programs under § 1030(a)(5)(A), and ***894** therefore violate the CFAA. [FN52] Thus, the placement of a defective disk controller software that allegedly caused damage to data on computers could violate the CFAA. "Time bomb" codes in certain cases can also violate the CFAA, though "time bomb" or other disabling codes that are part of a disclosed licensing arrangement would not likely fall within the CFAA. [FN53]

e. Setting of Cookies

The intentional placement of cookies on users' computers has been sufficient to establish intent under the CFAA, though the court ultimately concluded that the plaintiffs could not demonstrate any damage resulting from the placement of cookies. [FN54] Other courts have reached similar results regarding cookies, "action tags" and rerouting of users through other servers, all of which allegedly breached the users' web privacy. [FN55] Similarly, a pharmaceutical company's use of technology to obtain personal information from computers used to access websites did not constitute a violation of the CFAA because the users could not establish damage. [FN56]

f. Authorized Users Exceeding Scope of Authority

This category of claims is mainly connected with employees who exceed the scope of their authority. For example, the release of a computer "worm" on the Internet violated CFAA because, though the author had limited authority to access public Internet sites for communication purposes, his actions exceeded the scope of his authority. [FN57]

g. Illegal Subpoenas

The CFAA has been applied to litigants who have issued improper requests for information from ISPs. [FN58] In Theofel, a party ***895** requested all e-mails, without any limitation upon time or subject matter, from the opposing party's ISP. [FN59] The ISP provided a sample of e-mails to the requesting party, many of which were privileged. [FN60] The court held that an overbroad subpoena can constitute a violation of the CFAA, in

certain cases, because it exceeds the authorized access of the requesting party. [FN61]

h. Mere Review of Information

The mere review of information, even if not authorized, will not give rise to liability under the CFAA if the individual receives nothing of value. [FN62] In Czubinski, the defendant was an employee of the IRS that reviewed a number of individuals' personal tax data. Though the court acknowledged that the defendant had exceeded his authority when he reviewed tax payer's files, it concluded that his action were not done to gain anything of value but rather to fulfill his curiosity to see information about people he knew. [FN63]

i. Internet Advertising

Internet advertising has also served as the basis of a CFAA claim. Cases have been brought against a company that improperly accessed and copied data storage forms for Internet advertising services. [FN64] This conduct, because it allegedly resulted in the advertiser being forced to incur over $5,000 in assessment costs and corrective actions, was sufficient to allege a CFAA violation. [FN65]

3. State Computer Crime Laws

Over 40 states have computer crime laws that criminalize conduct in similar ways to the CFAA, though many do not have the “interruption in service” requirement. [FN66] A smaller subset of these laws provide civil remedies and therefore can also serve as a basis for ***896** privacy litigation. Examples of such laws are California Penal Code § 502 [FN67] and Virginia's computer crime laws. [FN68]

B. The ECPA

The Electronic Communications Privacy Act (ECPA) [FN69] consists of the Wiretap Act [FN70] and the Stored Communications Act. [FN71] The individual portions of the ECPA are sometimes referred to as Title I of the Act, the Wiretap Act, which exclusively applies to the interception of communications, and Title II, the Stored Communications Act, which applies to the dissemination or review of stored communications. [FN72] This is also a common claim made in privacy litigation. As with the CFAA, this law provides both civil and criminal remedies for violations. [FN73]

These acts regulate when electronic communications can be monitored or reviewed by third-parties, including ISPs. Generally, it is a crime for persons to intercept or procure electronic communications, [FN74] which include e-mails and other electronic messages and transmissions, unless certain exceptions apply. [FN75] These include: (1) if the communication is made through a system that is readily accessible to the general public; [FN76] (2) to protect the rights or property of the provider, although random monitoring cannot be done; [FN77] (3) if a provider of an electronic communication service reviews a communication to record the fact that a wire or electronic communication was initiated or completed if the purpose is to protect the provider, another provider, or a user, from fraudulent, unlawful or abusive use of the service; [FN78] (4) by court order; [FN79] (5) if the originator ***897** or addressee of any communication consents to the disclosure; [FN80] (6) a person employed or authorized, or whose facilities are used, to forward such communication to its destination (including employers); [FN81] or (7) if a communication is inadvertently obtained and the communication appears to pertain to the commission of a crime, if the communication is divulged to law enforcement. [FN82]

1. Temporal Distinctions

Title I only applies to conduct that occurs at the precise time of transmission. [FN83] This is in contrast to conduct that violates Title II, which relates to the improper acquisition of the contents of stored communications-i.e., after their transmission. [FN84] Thus, the difference between the two titles is a temporal one and Title I applies only to the interception or accessing of information while in transmission, while Title II applies to the unauthorized access of stored communications. [FN85]

2. Public versus Private Service Providers

Another important distinction created by the ECPA lies in its differing treatment of service providers that provide communication services to the "public" and those that do not. [FN86] "Public" service providers face additional hurdles when monitoring or disclosing communications. This is an important point for businesses, because an employer that simply provides e-mail or other Internet services to its employees would not be a service provider to the "public" and therefore faces lesser restrictions and exposure.

***898** 3. The Wiretap Act

Except as otherwise specifically provided under the ECPA, it is illegal for any person to: intentionally intercept; [FN87] endeavor to intercept; or procure any other person to intercept or endeavor to intercept, any wire, oral, [FN88] or electronic communication; [FN89] intentionally use, endeavor to use, or procure any other person to use or endeavor to use any electronic, mechanical, or other device [FN90] to intercept any oral communication when the device is affixed to, or transmits a signal through:

• a wire, cable, or other like connection used in wire communication; [FN91]

• the device transmits communications by radio, or interferes with the transmission of the communication;

• the person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce;

***899** • the use takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce;

• the purpose is to obtain information relating to the operations of any business or other commercial establishment of which affect interstate or foreign commerce; or

• the person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States. [FN92]

It is also illegal to intentionally disclose, or endeavor to disclose, the contents [FN93] of any wire, oral, or electronic communication, if the person knows, or has reason to know, that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this law. [FN94] Furthermore, it is illegal to intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, if the person knows or has reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this law. [FN95] Finally, it is a crime to intercept communications in order to interfere or impede a criminal investigation if certain specified conditions are met. [FN96]

Any person whose wire, oral or electronic communication is improperly intercepted, disclosed, or intention-

ally used in violation of this law may recover from the person or entity, other than the United States, that violated Title I any relief that may be appropriate. [FN97] The relief includes preliminary and other equitable or declaratory relief, damages, as set forth below, punitive damages in appropriate cases and reasonable attorneys' fees and other litigation costs reasonably incurred. [FN98] Agents of the United States, and the states, are exempt from liability. [FN99]

Actual or statutory damages are recoverable. Statutory damages range from $50 to $1,000 for certain violations (those that relate to ***900** viewing of select satellite or radio broadcasts for example). [FN100] For other violations, a court can award actual damages and any profits made by the violator, or statutory damages in the amount of $100 per day or $10,000-whichever is greater. [FN101]

4. Stored Communications Act

Except as set forth below, it is illegal to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in a system if a person intentionally accesses without authorization a facility through which an electronic communication service is provided. [FN102] It is also illegal to intentionally exceed an authorization to access that facility. [FN103]

a. Exceptions Permitting Disclosure

The Stored Communications Act does not apply to conduct authorized by the person or entity providing a wire or electronic communications service, or by a user of that service with respect to a communication of or intended for that user. [FN104]

A provider of electronic communication service may disclose the contents of a wire or electronic communication that is in electronic storage pursuant to a validly issued warrant if it is in storage for 180 days or less. [FN105]

If the communication is more than 180 days old, sent via electronic transmission [FN106] by a subscriber or customer of a remote computing service, [FN107] and was retained solely for the purpose of providing storage or computer processing services to the subscriber or customer, then the provider is not authorized to access the contents of the communications for purposes of providing any services other than storage or computer processing. [FN108] A government entity can require disclosure without notice to the subscriber or customer, if the ***901** governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure, or with notice if the government proceeds via a subpoena or grand jury subpoena, or under court order. [FN109]

b. Civil Damages

Any provider of electronic communication services, subscriber, or other person aggrieved by a violation of the Stored Communications Act may bring a civil action if it can show that the violation was known or intentional. [FN110] Available relief against any person or entity, other than the United States, includes preliminary and other equitable or declaratory relief, damages, punitive damages, reasonable attorneys' fees, and other reasonably incurred litigation costs. [FN111] Damages under the Stored Communications Act are the greater of actual damages and profits earned by the violator or $1,000. [FN112]

5. Examples of litigation under ECPA

In one of the early privacy cases, a plaintiff attempted to sue DoubleClick, Inc. for violations of the ECPA, CFAA, common law claims (including trespass to chattels), as well as a violation of New York's unfair competition laws. [FN113] DoubleClick challenged the propriety of the purported class action and won dismissal of the case. [FN114] The basis of the claim was the plaintiffs' assertion that DoubleClick had placed cookies on users' computers and collected data that included names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, web pages or sites visited on the Internet, and other communications and information that users would not ordinarily expect advertisers to be able to collect. [FN115] The plaintiffs alleged that these actions were taken without their consent and therefore gave rise to liability. [FN116]

In rejecting the theories advanced by the plaintiffs, the court noted that the ECPA violation failed for several reasons, including ***902** that DoubleClick's cookies were not temporary, and therefore did not fall within the statutory definitions of Title II, and that the websites that generated certain parts of the material were intended for these websites and those websites authorized DoubleClick's gathering of the information. [FN117]

Another common fact pattern that gives rise to litigation under ECPA is employee monitoring, and the Quon case provides an example of the issues in employee monitoring litigation. [FN118] The Quon case arose from the monitoring of employee communications on police department-provided pagers. [FN119] Two of the four plaintiffs (Jeff Quon and Steve Trujillo) were both police officers. [FN120] One of the other plaintiffs was a police dispatcher and the fourth was Jeff Quon's wife. [FN121] Jeff Quon and Steve Trujillo used department-provided pagers in the course and scope of their employment, and also allegedly used them for personal use, including sending sexually-explicit messages. [FN122] The department had a “general” policy of monitoring e-mail and other forms of communications, and also banned personal use of systems, but the policies were not read to explicitly cover text messaging. [FN123] Notably, Trujillo and Jeff Quon both signed the “general” policy, and both used the same form of technology-the department-provided pagers. [FN124]

However, only Jeff Quon attended later meetings, where the department allegedly stated that text messages were treated like e-mail and therefore covered by general policy. [FN125] There was also evidence of an informal policy to not monitor texting, which was evidenced by the fact that personal use was acknowledged and monitoring was not done unless the employee refused to pay for “excessive” personal use. [FN126]

***903** The provider in this case, Arch Wireless, kept a backup copy of the text messages. [FN127] Since it paid for the devices, the department was identified as the “subscriber” under the Stored Communications Act. [FN128] Based upon this conclusion, the department obtained copies of the content contained on the backup copy of the text messages from the service provider, without employee consent. The four plaintiffs sued, claiming that the disclosure of the content of communications violated the Stored Communications Act, their privacy rights, as well as other statutory protections. [FN129] The court initially examined the scope of the Stored Communications Act, and whether Arch Wireless was a “remote computing service” or an “electronic communication service,” because the answer to that question would impact whether the content of the communications could just be disclosed to the recipients, or also to the subscriber without the recipient's consent. [FN130] The court concluded that Arch Wireless was an electronic computing service and, as a result, it could not disclose the content of text messages to a subscriber without consent of a recipient. [FN131] Thus, Arch Wireless' disclosure to the department, the subscriber, according to the Ninth Circuit, violated the Stored Communications Act, and the employees' privacy rights. [FN132]

For three of the four plaintiffs, including Trujillo, the Ninth Circuit simply examined whether the users of text messaging have a reasonable expectation of privacy regarding text messages that are stored on the service

provider's network, ultimately concluding that there was a reasonable expectation of privacy, at least as to the service provider. [FN133] This expectation was not endless because the court noted that one of the recipients could have permitted the department to review the messages at issue. However, the court clearly stated that, as a matter of law, the plaintiffs had a reasonable expectation of privacy that the messages would not be reviewed absent the consent of a sender or recipient. Notably, even for Trujillo, who signed the same policy and used the same technology as Jeff Quon, the court did not apply the "general" policy. As a result, the ECPA claims were permitted to proceed.

***904** In the case of Jeff Quon, the only plaintiff who attended the meeting at which it was announced that the "general" policy covered texting, the Ninth Circuit examined the general policy, noting

> The Department's general "Computer Usage, Internet and E-mail Policy" stated both that the use of computers "for personal benefit is a significant violation of City of Ontario Policy" and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." Quon signed this Policy and attended a meeting in which it was made clear that the Policy also applied to use of the pagers. If that were all, this case would be analogous to the cases relied upon by the Appellees. [FN134]

The cases cited by the Appellees and referenced by theQuon court were all cases in which a policy defeated an employee's right of privacy, including theMuick case. [FN135] Thus, though both Trujillo and Jeff Quon signed the same policy, it was only applied to Jeff Quon because only he attended the meeting where the policy was applied to texting. [FN136]

However, these were not the only facts considered in the Quon case. Despite the application of the "general" policy to texting, the release of the text messages was still held to be improper because of the "operational reality" regarding texting. [FN137] The operational reality of the Department was that text messages were not monitored in most cases, particularly if personal use was paid for, and that many of the employees were aware of this fact. [FN138] Thus, despite having a policy on texting, the employer's failure to consistently implement it proved fatal and even Jeff Quon was permitted to continue his claim against Arch Wireless for violation of ECPA. [FN139]

6. State Wiretap Laws

Forty-nine states have statutory restrictions on wiretapping. All but 12 of these states closely track the requirements of ECPA, but there are 12 states that go beyond the federal requirements, particularly regarding the issue of two-party consent. A good example of litigation under state wiretap laws is the Kearney case. [FN140] In Kearney v. Salomon Smith Barney, Inc., the California Supreme Court ***905** determined the interaction of choice-of-law questions regarding California's wiretap act. [FN141] Unlike other states, including Georgia, California does not permit confidential communications to be recorded without the knowledge of all parties of the communication. [FN142] The defendant, a brokerage firm based in Georgia, was recording telephone calls without informing the other party. [FN143] This included communications with California consumers. [FN144]

The California Supreme Court concluded that, particularly in light of California's interest in protecting its residents, under California's choice-of-law doctrine, California law, not Georgia law, would control and thus rendered this practice illegal. [FN145]

C. CAN-SPAM

1. Establishing Liability Under CAN-SPAM

CAN-SPAM, like the Do-Not-Call and Do-Not-Fax laws, has privacy implications, in addition to restricting marketing. CAN-SPAM almost exclusively regulates emails that are “commercial” or are “transactional or relationship messages.” [FN146] Thus, one of the first issues in assessing the requirements of CAN-SPAM is to determine whether an e-mail is a “commercial” e-mail or it is a “transactional or relationship message.”

A commercial e-mail is one that has as its primary purpose commercial advertisement and/or the promotion of a commercial product or service. [FN147]A transactional or relationship message is one that:

• Facilitates, completes, or confirms a commercial transaction that the recipient has previously agreed to enter into with the sender;

• Provides warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

• For subscriptions, memberships, accounts, loans, or comparable ongoing commercial relationships involving the ***906** ongoing purchase or use by the recipient of products or services offered by the sender, an e-mail that provides:

(i) Notification concerning a change in the terms or features;

(ii) Notification of a change in the recipient's standing or status; or

(iii) At regular periodic intervals, account balance information or other type of account statement;

• To provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

• To deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender. [FN148]

While there are limited categories of e-mails that qualify as a transactional or relationship message, some portions of the law are read broadly. At least at the pleading stage, one court held that messages that fall within the exception of being “directly related to an employment relationship or related benefit plan” do not have to be sent by the actual employer. [FN149]

There are a number of litigation issues that arise under CAN-SPAM and state email laws, including whether there is sufficient “adverse effect” to state a claim, whether there is liability for the conduct of affiliates, the nature and type of remedies available, and the scope of CAN-SPAM's preemption of state law.

2. Actual harm Requirement

In order to state a claim under portions of CAN-SPAM, the electronic mail service provider must show that it was “adversely affected.” [FN150] Prior cases, including Hypertouch, held that this requirement was met when it was shown that high spam traffic caused ***907** network disruption and increased costs. [FN151] This is in contrast to cases such as Gordon v. Virtumundo, Inc. [FN152]

In Gordon, the plaintiff alleged he ran an ISP that had standing to bring a CAN-SPAM claim against the de-

fendants as a "provider of Internet access service adversely affected by a violation." [FN153] The defendants moved for summary judgment, claiming that the plaintiff did not have standing to bring the claim because it did not qualify as an adversely affected Internet Access Service. [FN154] As part of its analysis, the court noted the proliferation of these types of spam claims, which seek astronomical amounts of statutory damages, where little or no damage was suffered. [FN155] The court concluded that while in this case the plaintiffs might be able to show that they were an Internet Access Service, they could not show the necessary level of adverse effect. [FN156] This argument is frequently made by defendants against ISPs and typically defendants posit that ISPs must show a significant effect of a monetary or technical nature, directly caused by the e-mails at issue. This argument was soundly rejected by the District Court in the Northern District of California in ASIS Internet Services vs. Active Response Group. [FN157]

Most courts have found that ISPs, if they show harms that are unique to them, such as slowed networks and other similar harms, can state a claim under CAN-SPAM. [FN158] In Ferguson, the district court addressed whether an ISP had suffered sufficient harm to qualify under CAN-SPAM to state a civil cause of action. [FN159] The court noted that in order to be "adversely affected" an ISP had to show some costs ***908** or impact apart from what consumers suffer. [FN160] In this unique case, which did not involve a large commercial ISP, the plaintiff was unable to show he suffered adverse effect. [FN161] Indeed, in this case, he did not own a server, but "at best" rented service space. [FN162] In fact the court noted that any network harm would likely be borne by his server company, Sonic.net. [FN163] He also did not show he had to invest in new equipment or increase capacity or add new software due to the e-mails, nor did he show that he had to hire customer service personnel to deal with complaints. [FN164] At best, he showed that he had to switch from a dial up connection to a broadband connection, and this impact was insufficient to meet the adverse effect standard. [FN165]

3. Preemption

CAN-SPAM specifically preempts any state laws or regulations that expressly regulate the use of e-mail to send commercial messages. [FN166] However, state laws that regulate falsity or deception in e-mails are not preempted. CAN-SPAM does not explicitly affect any state laws that are not specific to e-mail, including state trespass, contract, or tort law. Finally, CAN-SPAM does not preempt laws that relate to acts of fraud or computer crime. However, this does not mean that CAN-SPAM does not impact these laws in certain ways.

Generally a court will begin any preemption analysis with two assumptions. First is the presumption that Congress did not intend to preempt the field of law. [FN167] Second, courts presume that the purpose of Congress is the "ultimate touchstone" in a case. [FN168] As such, preemption analysis does not seek to narrowly construe congressional intent, but rather seeks to fairly read the language, purpose, and structure of the statute at issue. [FN169]

One argument many plaintiffs have made is that an inaccuracy in an e-mail, however slight, renders the e-mail false or misleading, and ***909** therefore state law would not be preempted by CAN-SPAM in such a case. [FN170] This argument has been directly rejected by federal courts, because they have interpreted the false or misleading exception to preemption to require conduct equivalent to fraud. [FN171]

There are three types of preemption: express, field, and conflict preemption. "Express preemption occurs when Congress has considered the issue of preemption, has included in the legislation under consideration a provision expressly addressing that issue, and has explicitly provided therein that state law is preempted." [FN172]

When Congress has expressly defined the extent to which state law is preempted, a court will inter-

pret the effect of the preemption language by focusing on the plain wording of the provision, but will narrowly construe the precise language of the preemption clause in light of the strong presumption against preemption." [FN173]

Thus, where Congress expressly intended to preempt state law, the state law is of no effect.

However, there are other forms of preemption that are implicated by CAN-SPAM: conflict preemption and obstacle preemption. It is well-settled that state law that conflicts with federal law is "without effect." [FN174] Conflict preemption occurs when it is impossible for a private party to comply with both federal and state law. [FN175] Obstacle preemption occurs when, under the circumstances of a particular case, the challenged state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress. [FN176] As stated by the United States Supreme Court: "[w]hat is a sufficient obstacle is a matter of judgment, to be informed by examining the federal statute as a whole and identifying its purpose and intended effects." [FN177] Thus, in certain cases, conflicting state e-mail, or other, laws may be preempted by CAN-SPAM even though the law is not expressly preempted, particularly if the law in question would stand ***910** as an obstacle to the accomplishment and execution of the congressional objectives behind CAN-SPAM.

One area where this issue has been addressed is the preemptive effect of CAN-SPAM on state university e-mail policies. [FN178] The university in White Buffalo had adopted certain regulations that precluded the plaintiff from sending certain e-mails through the university system. [FN179] The issue ultimately involved a decision as to whether the university was acting as a state actor, or as a service provider. Ultimately the court concluded that while there was preemption language that supported both sides, the university's restrictions as a service provider were valid under the Supremacy Clause. [FN180]

The District Court in the Central District of California addressed the level of fraud required to escape CAN-SPAM preemption, holding that common law fraud, including reliance, was required, and the mere failure to include a company name in an e-mail would not be considered a sufficient showing to defeat preemption by alleging fraud, citing the legislative history of CAN-SPAM and its direction that states not force e-mails to contain certain content. [FN181]

D. Federal Do-Not-Call law

1. The Requirements of Do-Not-Call

The federal Do-Not-Call law [FN182] is generally viewed as one of the more successful attempts to protect consumer privacy. Though it is framed in the terms of restrictions on marketing activity, it is truly a privacy statute that is simply specific to a method of communicating certain messages. The hallmark of the law is the Do-Not-Call list, [FN183] an opt-in list on which consumers can place themselves. This act by a consumer precludes many forms of telephone communications, particularly those that promote commercial services, unless there is a pre-existing relationship between the business and the consumer. Do-***911** Not-Call laws also have record retention requirements, as well as disclosure requirements in many cases.

Many states have followed the federal government's lead and enacted their own laws, which are in large part driven by the existence of the Do-Not-Call registry. [FN184] These laws also can contain restrictions on the use of prerecorded messages, and these restrictions may not be contained in the same section of the code in which the Do-Not-Call law was placed. [FN185] Indeed, some states have placed restrictions on recorded messages and auto-dialers in the Public Utilities Code. [FN186] It should be noted that certain state laws actually regulate

direct mail and other written solicitations under their Do-Not-Call laws if the writing attempts to solicit a call. In order to ensure compliance, a review of applicable state laws is frequently required. [FN187]

It is a violation of the Do-Not-Call law [FN188] if a telemarketer [FN189] or a seller [FN190] causes a telemarketer to cause any telephone to ring, or to engage any person [FN191] in telephone conversation, repeatedly or continuously with intent to annoy, abuse, or harass any person at the called number, or deny or interfere in any way, directly or indirectly, with a person's right to be placed on any registry of names and/or telephone numbers of persons who do not wish to receive outbound telephone calls. [FN192] It is also improper to initiate an outbound call when that person previously has stated that he or she does not wish to receive an outbound telephone call made by or on behalf of the seller whose goods or services are being offered or made on behalf of the charitable organization for which a charitable contribution [FN193] is being ***912** solicited, or that person's telephone number is on the "do-not-call" registry, maintained by the Commission, of persons who do not wish to receive outbound telephone calls to induce the purchase of goods or services unless the seller:

• has obtained the express agreement, in writing, of such person to place calls to that person. Such written agreement shall clearly evidence such person's authorization that calls made by or on behalf of a specific party may be placed to that person, and shall include the telephone number to which the calls may be placed and the signature, including a valid electronic signature, of that person; or

• has an established business relationship [FN194] with such person, and that person has not stated that he or she does not wish to receive outbound telephone calls under the above-referenced portions of this rule. [FN195]

It is also an illegal act to abandon [FN196] an outbound call, [FN197] to sell, rent, lease, purchase, or use any list established to comply with the Do-Not-Call list for any purpose except compliance with the provisions of this Rule, or otherwise to prevent telephone calls to telephone numbers on such lists. [FN198]

It is also improper if the seller and/or telemarketer is initiating any outbound telephone call that delivers a prerecorded message, other than a prerecorded message permitted for compliance with the call abandonment safe harbor in § 310.4(b)(4)(iii), unless in any such call to induce the purchase of any good or service, the seller has obtained from the recipient of the call an express agreement, in writing, that:

• the seller obtained only after a clear and conspicuous disclosure that the purpose of the agreement is to authorize the seller to place prerecorded calls to such person;

***913** • the seller obtained without requiring, directly or indirectly, that the agreement be executed as a condition of purchasing any good or service;

• evidences the willingness of the recipient of the call to receive calls that deliver prerecorded messages by or on behalf of a specific seller; and

• includes such person's telephone number and signature. [FN199]

Additionally, in any such call to induce the purchase of any good or service, or to induce a charitable contribution from a member of, or previous donor to, a non-profit charitable organization on whose behalf the call is made, the seller or telemarketer also must allow the telephone to ring for at least 15 seconds or 4 rings before disconnecting an unanswered call; and within 2 seconds after the completed greeting of the person called, plays a prerecorded message that promptly provides the disclosures required by § 310.4(d) or (e), followed immedi-

ately by a disclosure of one or both of the following: in the case of a call that could be answered in person by a consumer, that the person called can use an automated interactive voice and/or keypress-activated opt-out mechanism to assert a Do-Not-Call request pursuant to § 310.4(b)(1)(iii)(A) at any time during the message. [FN200] The mechanism must automatically add the number called to the seller's entity-specific Do-Not-Call list, once invoked, immediately disconnect the call, be available for use at any time during the message, and in the case of a call that could be answered by an answering machine or voicemail service, that the person called can use a toll-free telephone number to assert a Do-Not-Call request pursuant to § 310.4(b)(1)(iii)(A). [FN201] The number provided must connect directly to an automated interactive voice or keypress-activated opt-out mechanism that: automatically adds the number called to the seller's entity-specific Do-Not-Call list; immediately thereafter disconnects the call; and is accessible at any time throughout the duration of the telemarketing campaign. [FN202]

***914** 2. Federal Do-Not-Call Defenses

It is a defense to any action for a violation of these provisions if the seller or telemarketer can demonstrate that, as part of the seller's or telemarketer's routine business practice:

(1) It has established and implemented written procedures to comply with 16 C.F.R. §§310.4(b)(1)(ii) and (iii);

(2) It has trained its personnel, and any entity assisting in its compliance, in the procedures established pursuant to 16 C.F.R. §310.4(b)(3)(i);

(3) The seller, or a telemarketer or another person acting on behalf of the seller or charitable organization, has maintained and recorded a list of telephone numbers the seller or charitable organization may not contact, in compliance with 16 C.F.R. §310.4(b)(1)(iii)(A);

(4) The seller or a telemarketer uses a process to prevent telemarketing [FN203] to any telephone number on any list established pursuant to 16 C.F.R. §310.4(b)(3)(iii) or 16 C.F.R. §310.4(b)(1)(iii)(B), employing a version of the "do-not-call" registry obtained from the Commission no more than 31 days prior to the date any call is made, and maintains records documenting this process;

(5) The seller or a telemarketer or another person acting on behalf of the seller or charitable organization, monitors and enforces compliance with the procedures established pursuant to §310.4(b)(3)(i); and

(6) Any subsequent call otherwise violating §310.4(b)(1)(ii) or (iii) is the result of error. [FN204]

There is similarly no liability for abandoning calls if:

***915** • the seller or telemarketer employs technology that ensures abandonment of no more than 3% of all calls answered by a person, measured per day per calling campaign, if less than 30 days, or separately over each successive 30-day period or portion thereof that the campaign continues;

• the seller or telemarketer, for each telemarketing call placed, allows the telephone to ring for at least 15 seconds or 4 rings before disconnecting an unanswered call;

• whenever a sales representative is not available to speak with the person answering the call within 2 seconds after the person's completed greeting, the seller or telemarketer promptly plays a recorded message that

states the name and telephone number of the seller on whose behalf the call was placed; and

• the seller or telemarketer, comply with the record retention requirements. [FN205]

There are also a number of other, additional, restrictions and requirements contained in the regulations that implement the TCPA.

3. TCPA litigation issues

While certain other sections of the TCPA have been held to create a private right of action to enforce certain requirements, the regulations that implement §227(d), including the requirement to have identifying information, do not give rise to a private right of action, as does §227(b), or presumably the regulations promulgated under that section. [FN206]

Federal courts have routinely found that jurisdiction for TCPA claims exist only in state court. [FN207] Illinois has also recently held that a ***916** private right of action exists under the TCPA. [FN208] Moreover, a district court in Ohio recently concluded that the TCPA did not create jurisdiction in federal court under federal question jurisprudence. [FN209]

4. California “Do Not Call” List

Not to be left out, many states have enacted their own Do-Not-Call laws. Under California law it is unlawful for any person to do any of the following: using the “do not call” list for any purpose other than to comply with this article or applicable federal laws; denying or interfering in any way, directly or indirectly, with a subscriber's right to place a California telephone number on the “do not call” list; causing a subscriber to participate in and be included on the “do not call” list without the subscriber's knowledge or consent; selling or leasing the “do not call” list to a person other than a telephone solicitor; selling or leasing by a telephone solicitor of the “do not call” list; charging a fee to place a California telephone number on the “do not call” list; and a telephone solicitor, either directly or indirectly, persuading a subscriber with whom it has an established business relationship to place his or her telephone number on the “do not call” list, if the solicitation has the effect of preventing competitors from contacting that solicitor's customers. [FN210]

5. Civil Enforcement

The Attorney General, a district attorney, or a city attorney may bring a civil action in any court of competent jurisdiction against a telephone solicitor to enforce the article and to obtain any one or more of the following remedies: an order to enjoin the violation; a civil penalty of up to the penalty amount that the Federal Trade Commission may seek pursuant to subparagraph (A) of paragraph (1) of subsection (m) of Section 45 of Title 15 of the United States Code as specified in Section 1.98 of Title 16 of the Code of Federal Regulations; or any other relief that the court deems proper. [FN211]

Any person who has received a telephone solicitation that is prohibited by § 17592, or whose telephone number was used in violation of § 17591, may bring a civil action in small claims court for ***917** an injunction or order to prevent further violations. [FN212] If a person obtains an injunction or order under this subdivision and service of the injunction or order is properly effected, a person who thereafter receives further solicitations in violation of the injunction or order within 30 days after service of the initial injunction or order, may file a subsequent action in small claims court seeking enforcement of the injunction or order and a civil penalty to be

awarded to the person in an amount up to $1,000. [FN213] For purposes of this subdivision, a person's claims may not be aggregated to establish jurisdiction in a court other than small claims court. [FN214] For purposes of this subdivision, a defendant is not required to personally appear, but may appear by affidavit or by written instrument. [FN215] The rights, remedies, and penalties established by this article are in addition to the rights, remedies, or penalties established under other laws. [FN216]

It is an affirmative defense to any action brought under this article that the violation was accidental and in violation of the telephone solicitor's policies and procedures and telemarketer instruction and training. [FN217]

6. Nondisclosure of information

Any information regarding any California telephone number which appears on the “do not call” list in the possession of the Attorney General, whether obtained from the Federal Trade Commission or submitted to the Attorney General by a subscriber for inclusion in the “do not call” list, shall not be disclosed pursuant to a request made under Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code and shall also be privileged under Section 1040 of the Evidence Code. [FN218] Notwithstanding the foregoing, nothing in this section prevents the Attorney General from providing a certificate stating whether a specific telephone number was on the “do not call” list that was effective on the specified date or range of dates in response to: an inquiry from any law enforcement agency that is investigating, prosecuting, or responding to an allegation of a violation of this ***918** article; or an inquiry from an individual who is investigating or litigating an alleged violation of this article and who seeks the certificate regarding his or her telephone number or to an inquiry from the person who is responding to the allegation. [FN219]

E. Federal Do-Not-Fax law

Do-Not-Fax laws also exist, and follow a similar model to the Do-Not-Call laws. Under the federal statute, it is improper to use any telephone facsimile machine, [FN220] computer, or other device to send to a telephone facsimile machine an unsolicited advertisement, [FN221] unless:

(1) the unsolicited advertisement is from a sender with an established business relationship [FN222] with the recipient;

(2) the sender obtained the number of the telephone facsimile machine through the voluntary communication of such number, within the context of such established business relationship, from the recipient of the unsolicited advertisement, or a directory, advertisement, or site on the Internet to which the recipient voluntarily agreed to make available its facsimile number for public distribution. [FN223]

This restriction does not apply if such a fax is sent based upon an established business relationship with the recipient that was in existence before July 9, 2005, if the sender possessed the facsimile machine number of the recipient before such date of enactment, and ***919** the unsolicited advertisement meets the notice requirements identified below. [FN224]

It should be noted that this exception does not apply when the consumer has expressly opted-out of receiving such communications. [FN225]

1. Do-Not-Fax-the established business relationship in the business context

One argument that was made by plaintiffs in the do-not-fax context was that the established business relationship exception to the Do-Not-Fax law did not include businesses. [FN226] This argument has been rejected, though review of the decision has been granted by the California Supreme Court. [FN227]

2. Federal Do-Not-Fax law-Opt-outs

Any unsolicited advertisement that is sent via fax must contain a clear and conspicuous disclosure on the first page of the advertisement that states that the recipient may request that the sender of the unsolicited advertisement not send any future unsolicited advertisements to a telephone facsimile machine or machines. [FN228] It must also disclose that the failure to comply, within the shortest reasonable time, as determined by the FTC, is unlawful. [FN229] The notice must also contain a domestic contact telephone and facsimile machine number for the recipient to transmit such a request to the sender and a cost-free mechanism for a recipient to transmit an opt-out request. [FN230] The telephone and facsimile machine numbers and the cost-free mechanism must permit an individual or business to make such a request at any time on any day of the week. [FN231]

In order to be effective, the opt-out must identify the telephone number or numbers of the telephone facsimile machine or machines to which the request relates, the request must be made to the ***920** telephone or facsimile number of the sender of such an unsolicited advertisement provided above, or by any other method of communication as determined by the Commission, and the person making the request has not, subsequent to such request, provided express invitation or permission to the sender, in writing or otherwise, to send advertisements to the person at the telephone facsimile machine. [FN232]

A private right of action, including statutory penalties, is permitted by the law.

F. Lanham Act

In CollegeNet, Inc., the Lanham Act was used by a competitor to litigate issues regarding online privacy policies. [FN233] CollegeNet is a company that provides online college admission application services to applicants. CollegeNet received payments from colleges for its services. [FN234]

XAP was alleged to be a competitor of CollegeNet who provided similar services through “Mentor” Websites. [FN235] XAP allegedly did not receive payment from the colleges, but rather from certain state agencies, as well as other commercial institutions, such as banks and other lending organizations. XAP's website contained a privacy policy that stated that personal data would not be shared with third-parties without the user's “express consent and direction.” [FN236] The privacy policy also stated that “[t]he information you enter will be kept private in accordance with your express consent and direction.” [FN237]

Certain XAP web pages asked an opt-in question of the applicants, which was, in essence, were they interested in receiving information about student loans or financial aid. [FN238] If a customer answered yes, their information was provided to the lending institutions that were the defendant's paying customers. [FN239] There was allegedly no express disclosure that by answering yes to this question information would be shared with third-parties.

***921** CollegeNet asserted that XAP had engaged in unfair competition under the Lanham Act by falsely representing its privacy policy to consumers, and moved for summary judgment on its claims of unfair competition. [FN240] XAP disputed this and also moved for summary judgment. [FN241] XAP first argued that these state-

ments were merely incidental, and not fundamental, to its products and services and therefore not actionable. [FN242] The court rejected this argument, finding that Internet privacy promises are not "minor matters." [FN243] While the court did not determine that the statements were "literally untrue," the court concluded that there was sufficient evidence to permit the claim to proceed past the summary judgment and go to trial on this, and other issues. [FN244] The court also found that there was sufficient evidence to deny summary judgment on the grounds that the statements were potentially material to the defendant's customers, notably not the consumers, but rather the financial institutions that paid the defendant. [FN245]

G. California Law-Business and Professions Code § 17200

State unfair competition laws in many cases mirror the FTC Act, and California's law [FN246] has been brought more in line with the FTC Act. California's statute proscribes unfair competition and deceptive acts or practices, as well as false advertising. [FN247] The California Attorney General, certain county attorneys, and private citizens all can bring claims under Section 17200. [FN248] Representative actions are also permitted under this law, although this has been dramatically reduced. [FN249] Now the lead plaintiff must allege actual injury, [FN250] which in these cases, as noted below, can be difficult.

A 17200 claim is commonly made by plaintiffs and the cause of action has been included in privacy related litigation. [FN251] Moreover, as ***922** unfair competition claims, such as the claim made in CollegeNet, Inc., become more common, 17200 may become a central claim in plaintiffs' privacy litigation. The UCL's statutory origins are California's codification of nuisance laws. [FN252] As the federal government increasingly regulated corporate conduct via statutes administered by the FTC, California similarly increased the UCL's scope. [FN253] Primarily due to a series of statutory amendments that occurred in the 1990's, the UCL expanded far beyond the FTC Act, though recent amendments have somewhat restricted its scope. [FN254]

The UCL regulates five forms of conduct: unlawful; unfair, or fraudulent business practices; unfair, deceptive, untrue or misleading advertising; and any act prohibited under Business and Professions Code Sections 17500-17577.5. [FN255] While these categories might, at first blush, appear to be quite narrow, in reality the UCL has a broad sweep and has been utilized in numerous contexts. Indeed, the UCL's breadth and impact are apparent from its use in a wide variety of cases, ranging from individuals seeking redress for the alleged improper payment of rather insignificant account fees, [FN256] to a consumer group bringing an action to stop the alleged sale of cigarettes to minors, [FN257] to a competitor seeking disgorgement of profits wrongfully obtained by another competitor, amounting to approximately $30 million. [FN258]

One of the most complex issues facing defendants in UCL claims is the scope of relief available to a plaintiff. [FN259] Section 17203 is the only statutory provision that provides guidance on the issue of available remedies under the UCL. [FN260] Under this provision, any ***923** person who engages, has engaged, or proposes to engage in unfair competition may be enjoined by any court of competent jurisdiction. Section 17203 states that:

> [a]ny person who engages, has engaged, or proposes to engage in unfair competition may be enjoined in any court of competent jurisdiction. The court may make such orders or judgments, including the appointment of a receiver, as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition, as defined in this chapter, or as may be necessary to restore to any person in interest any money or property, real or personal, which may have been acquired by means of such unfair competition. [FN261]

Section 17203 has been interpreted as giving courts broad remedial powers in order to effectuate the purpose of the statute. [FN262] Thus, courts have utilized their authority to design appropriate relief in a variety of circumstances. [FN263]

A court can grant injunctive relief as well as other forms of equitable relief, including appointing a receiver. [FN264] Courts are also authorized to "restore" to any person any money or property which was acquired by unfair competition. In other words, the equitable remedy of restitution [FN265] is expressly permitted. Finally, civil penalties are authorized in certain circumstances under Section 17203. [FN266]

However, courts have held that restitution does not equate to other more traditional forms of compensatory, or monetary, damages that are available in other claims. These damages include lost profits and other forms of relief to compensate the plaintiff for harms it suffered and to restore equity. [FN267] Several federal courts interpreted the language of Section 17203 as precluding the recovery of damages. [FN268] ***924** The California Supreme Court ended this debate in 1992 when it held that damages are not available under the UCL. [FN269]

The California Supreme Court has now held that only restitution, and not disgorgement, is available as a remedy under the unfair competition law. [FN270] Thus, as a condition to recovery of restitution, the plaintiff must show that the defendant gained funds directly from the plaintiff, and not profits that came from a third-party. [FN271]

H. California law-Civil Code § 1747.08

California, as part of its credit card laws, has restricted the collection of certain information in connection with a credit card transaction and this law has been a common basis of privacy litigation, including class actions in California.

Except as otherwise provided, no person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall do any of the following: request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to write any personal identification information [FN272] upon the credit card transaction form or otherwise; request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise; or utilize, in any credit card transaction, a credit card form which contains preprinted spaces ***925** specifically designated for filling in any personal identification information of the cardholder. [FN273]

These restrictions do not apply: if the credit card is being used as a deposit to secure payment in the event of default, loss, damage, or other similar occurrence; to cash advance transactions; if the person, firm, partnership, association, or corporation accepting the credit card is contractually obligated to provide personal identification information in order to complete the credit card transaction or is obligated to collect and record the personal identification information by federal law or regulation; or if personal identification information is required for a special purpose incidental but related to the individual credit card transaction, including, but not limited to, information relating to shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders. [FN274]

This law does not prohibit any person, firm, partnership, association, or corporation from requiring the card-

holder, as a condition to accepting the credit card as payment in full or in part for goods or services, to provide reasonable forms of positive identification, which may include a driver's license or a California state identification card, or where one of these is not available, another form of photo identification, provided that none of the information contained thereon is written or recorded on the credit card transaction form or otherwise. [FN275] If the cardholder pays for the transaction with a credit card number and does not make the credit card available upon request to verify the number, the cardholder's driver's license number or identification card number may be recorded on the credit card transaction form or otherwise. [FN276]

1. Civil Enforcement

Any person who violates this law is subject to a civil penalty not to exceed $250 for the first violation and $1,000 for each subsequent violation, to be assessed and collected in a civil action brought by the person paying with a credit card, by the Attorney General, or by the district attorney or city attorney of the county or city in which the violation occurred. [FN277] However, no civil penalty may be assessed for a ***926** violation of this section if the defendant shows by a preponderance of the evidence that the violation was not intentional and resulted from a bona fide error made notwithstanding the defendant's maintenance of procedures reasonably adopted to avoid that error. [FN278] When collected, the civil penalty shall be payable, as appropriate, to the person paying with a credit card who brought the action, or to the general fund of whichever governmental entity brought the action to assess the civil penalty. [FN279]

The Attorney General, or any district attorney or city attorney within his or her respective jurisdiction, may bring an action in the superior court in the name of the people of the State of California to enjoin violation of these restrictions and, upon notice to the defendant of not less than 5 days, to temporarily restrain and enjoin the violation. [FN280] If it appears to the satisfaction of the court that the defendant violated these restrictions, the court may issue an injunction restraining further violations, without requiring proof that any person has been damaged by the violation. [FN281] In these proceedings, if the court finds that the defendant has violated these restrictions, the court may direct the defendant to pay any or all costs incurred by the Attorney General, district attorney, or city attorney in seeking or obtaining injunctive relief pursuant to this subdivision. [FN282]

2. Zip codes and § 1747.08

One argument plaintiffs have made is that a zip code is personal identification information under the definition of this statute. [FN283] In a recent case the Appellate Court concluded that a zip code is not itself specific or personal information about an individual, but rather it serves as a group identifier about location, and was therefore not personal identification information under this law, holding that “Plaintiff is painting with too broad a brush to state that under the Act, any component of an address is necessarily a ‘personal identification’ item, since the zip code portion of an address does not in itself supply enough information to identify an individual.” [FN284]

***927** 3. Other litigation issues under § 1747.08

Plaintiffs have attempted to expand the amount of litigation under this law to include Internet transactions, and returns of merchandise and these efforts have been thwarted. [FN285]

I. Privacy litigation-Electronic conversion

New York, among other states, has now recognized a conversion claim for electronic data. [FN286] Certain other courts have permitted trespass to chattels claims to be stated based upon improper pop-up advertising. [FN287] Other courts have rejected a finding that electronic data can serve as the basis of a conversion claim. [FN288]

V. Damages in Privacy Litigation

Private plaintiffs, where their claims rely upon statutes or theories that do not include statutory damages, have faced dismissal of their claims in many cases because they either lack standing to bring their claim, or cannot prove that compensable damages resulted from the alleged privacy breach. In Trikas, one of the first of such cases, the court rejected a plaintiff's claim for violation of the Fair Credit Reporting Act. [FN289] The plaintiff brought an action based upon the assertion that an account erroneously remained open on his credit report, [FN290] claiming that he had suffered emotional distress because of this, even though it was admitted that no creditor actually saw or relied upon the erroneous information. [FN291]

***928** There have been several recent cases that have addressed the issue of whether the breach of a privacy policy can support litigation against a party that did not comply with its own policy. Courts have concluded that the mere breach of a privacy policy may not be sufficient to establish a claim for damages. In Dyer, [FN292] a group of plaintiffs sued Northwest Airlines for allegedly disclosing personal information gathered via the Web to certain government agencies in direct violation of Northwest's posted privacy policy. [FN293] Northwest advanced two theories to defeat the plaintiffs' claims. First, it argued that its online policy was not a contract, but rather an aspirational policy, the violation of which did not give rise to contractual liability. [FN294] Second, Northwest Airlines argued that even assuming its act was a breach of contract, the plaintiffs could not show any damage that resulted from the disclosure. [FN295] The court accepted both arguments and dismissed the plaintiffs' claims, finding that there was no breach of contract for several reasons, including a lack of damages. [FN296]

In Stollenwerk, [FN297] the Arizona district court addressed issues related to causation and the speculative nature of damages arising out of privacy breaches, even where indisputably certain identity theft issues had occurred. Tri-West maintained personal information regarding a number of current and former members of the U.S. Military, as well as their dependents, and had experienced security breaches where unauthorized personnel entered their facilities. [FN298] The plaintiffs alleged that despite this event, another breach occurred when hard drives, containing plaintiffs' personal information, were stolen from the same facility. [FN299] One of the plaintiffs had six credit accounts opened under his name. [FN300] Some of the plaintiffs did not suffer identity theft, but they incurred costs in connection with ***929** obtaining certain reports regarding their credit, as well as identity theft insurance. [FN301]

While the court noted that identity theft issues could frequently result in damages other than purely pecuniary damages, this was insufficient to state a claim for negligence, even though psychological or emotional distress, inconvenience and harm to credit rating or reputation could occur. [FN302] The plaintiffs attempted to avoid dismissal by arguing that privacy breach cases were akin to toxic torts since a privacy breach, in the plaintiffs' mind, could lead to increased chance of identity theft. Since toxic tort cases in certain instances find that medical monitoring costs can be damage, the plaintiffs argued that their claims should not be dismissed. [FN303] The court soundly rejected this argument [FN304] by deciding that even though one of the plaintiffs had experienced credit issues, the court held that there was insufficient evidence showing that it was caused by

the theft of hard drives and dismissed his claim as well. [FN305]

The Ninth Circuit reviewed this decision and, in an unpublished opinion, modified the analysis. While it still upheld the dismissal of two of the three plaintiffs' claims, and completely rejected the medical monitoring analogy, it reversed the judgment in favor of the third plaintiff, finding that given the unique factual circumstances there could be potential damages that flowed from the alleged disclosure of information. [FN306] It therefore reversed in part, affirmed in part, and remanded the case. [FN307]

The court in Forbes reached a similar conclusion. [FN308] In this case, the plaintiffs' personal information was obtained through a theft of computers that contained unencrypted customer information including names, addresses, social security numbers and account numbers. [FN309] Again, it was undisputed that plaintiffs had expended time and money to monitor credit, but there was no indication that the information had ***930** been accessed or misused. [FN310] Consistent with the other decisions cited above, the court rejected the plaintiffs' claim that they had suffered damage as a result of the time and money they had spent to monitor their credit, because the plaintiffs could not prove a loss of earning capacity or wages. [FN311] The court therefore rejected both the breach of contract and negligence claims.

Similar conclusions have been reached by other courts, including in the DSW matter. [FN312] Recently, in Kahle, an Ohio court followed the DSW decision by finding that economic harm was a prerequisite for a plaintiff to state a claim for damages. [FN313] Kahle concerned a security breach that could have resulted in the disclosure of the plaintiff's personal information. [FN314] The defendant advised all affected individuals to place a credit freeze on their report. [FN315] The plaintiff could not establish any direct damages, other than costs associated with a credit monitoring service that the plaintiff purchased. [FN316] The court dismissed the claim, holding that any alleged damages were too speculative, particularly since the defendant had advised the plaintiff to place a security freeze on her credit report. [FN317] The court dismissed the claim despite the fact that the plaintiff was seeking reimbursement of monies paid for a credit monitoring service. In addition to this case, courts are still routinely finding that damages resulting from future identity theft are too speculative to be the basis of a successful civil claim. [FN318] The lack of damages issue has also been addressed in the context of FCRA, at least for claims of actual damages. [FN319] FCRA does, however, permit recovery of statutory damages for willful ***931** violations, and claims without damages can, sometimes, survive. [FN320] This was also the conclusion in cases involving American Airlines and JetBlue. [FN321]

VI. Standing in Privacy Litigation

Standing is a related issue to damages, though some courts continue to reach conclusions regarding standing that are inconsistent with their findings of no actual damages. Standing is a constitutional issue under Article III, and the party invoking federal jurisdiction bears the burden of establishing the following three elements: that it has suffered an injury in fact-an invasion of a legally-protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical; a causal connection between the injury and the conduct complained of-the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court; and that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. [FN322]

Article III's requirements are not “mere” pleading formalities. They are “rather an indispensable part of the plaintiff's case, [and] each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the

litigation." [FN323] Irrespective of other laws to the contrary, Article III standing is the "irreducible constitutional minimum" of standing and a "threshold issue" to be addressed before a federal court "proceeds at all in any cause." [FN324] Because it is a jurisdictional issue, Article III standing can be challenged at any point in the case or raised sua ***932** sponte by federal courts. [FN325] It is against this backdrop that cases regarding standing must be viewed.

In Bell v. Acxiom, the court addressed the issue of damages in a privacy case arising out of a computer hacking incident and the plaintiff's lack of standing was an issue raised by the defendant. The plaintiff alleged that the hacking incident compromised her personally identifiable information and that "lax security" left her at risk for privacy issues, as well as receiving junk mail. [FN326] The main issue addressed was whether the plaintiff had standing to pursue the claim. In this case, because the plaintiff could not show injury, or even that she received any junk mail, the court dismissed her case because she lacked standing. [FN327]

A court recently reaffirmed the principle that damage did not occur, and therefore no standing existed, at the time of a data theft in the absence of evidence of harm. [FN328] The court distinguished cases from Ohio that did find harm at the moment of disclosure when the disclosure involved medical information. [FN329] It also distinguished cases ***933** involving the disclosure by the government of Social Security numbers. [FN330]

In the Pichler, case the Third Circuit considered whether the DPPA applied to union activities, but more importantly addressed standing in privacy litigation. [FN331] In this case a union gathered license plates at a company and then bought information related to the license plates in an effort to identify targets for unionizing activity. [FN332] Within the plaintiff group were spouses of the registered owners of vehicles and the non-owner spouses' information was revealed within the searches. [FN333] The court held that since the spouses were not registered owners (and therefore not identified in the records) of automobiles they lacked standing to bring a claim under the DPPA. [FN334] The court rejected the argument that these plaintiffs had standing because they shared an address with individuals covered by the DPPA. [FN335]

Despite these holdings, and the clear mandate of Lujan, some courts have found that plaintiffs have Article III standing in data loss cases, despite an often concurrent finding that the plaintiff cannot prove damage. [FN336] Pisciotta involved allegations of data loss and the Seventh Circuit, though it recognized many courts reached a different conclusion, first ruled that the allegations of data loss were sufficient to establish standing to assert negligence and breach of contract cases. [FN337] It then, dismissed the plaintiffs' case, finding that the plaintiffs could not establish damages, a required element of its ***934** negligence and breach of contract claims, and therefore dismissed the case. [FN338]

This case was applied by the Southern District of New York in another loss data case resulting from the theft of computers. [FN339] As in Pisciotta, the District Court in Caudle found that allegations of lost data in this case were sufficient to meet the plaintiff's standing burden. [FN340] Pisciotta was also recently followed in this case arising from an alleged security breach involving the Gap. [FN341] In this case, the plaintiff alleged that the Gap, via a third-party, had lost data regarding a class of individuals due to a laptop computer theft. [FN342] The District Court examined whether the plaintiff had standing, finding that the plaintiff had met his burden. The court then examined whether the plaintiff could state a claim against the Gap, finding that the plaintiff could not state a breach of contract or negligence claim. "While Ruiz has standing to sue based upon his increased risk of future identity theft, this risk does not rise to the level of appreciable harm necessary to assert a negligence claim under California law." [FN343]

These holdings highlight the fact that Article III standing does not exist since the courts inconsistently find that plaintiff's have met their burden under standing, but fail as a matter of law to meet their evidentiary burden to state a claim. Indeed, the clear mandate of Lujan requires he plaintiff meet his burden of proof "with the manner and degree of evidence required at the successive stages of the litigation." [FN344] Since these courts are simultaneously finding sufficient injury exists for Article III, but also finding the plaintiffs have failed to meet their burden of proof to establish a claim, the analysis of the Bell v. Acxiom line of cases appears to be more consistent with Lujan.

VII. Immunity in Litigation-The Communications Decency Act

The Communications Decency Act offers some level of immunity to defendants that face privacy litigation, though most of the litigation regarding the CDA has taken place regarding other ***935** issues. [FN345] The goal of the Communications Decency Act (CDA) was to promote the growth of the Internet, to encourage restrictions on improper content and, at the same time, limit the liability of ISPs for publishing statements that were authored by third-parties. [FN346] One of the underlying themes of laws regarding the Internet, as well as the cases interpreting them, is that the Internet was so delicate that it could be destroyed by the heavy-handed regulation of legislatures and courts. This thinking underlies the CDA, the Internet tax debate, as well as many other issues. Now, from the Ninth Circuit, we see the first decision that questions this underlying theory, and instead posits a theory that online commerce should not gain certain benefits over offline activity. [FN347]

The CDA was passed by Congress in response to a particular case, Stratton Oakmont, Inc. v. Prodigy Services Co., which held an Internet Service Provider liable for defamation due to messages placed upon a message board it ran. [FN348] The basis of that court's ruling was that Prodigy exercised editorial control over the messages because it selectively deleted certain messages, and not others. [FN349] The Ninth Circuit recently summarized the purpose of the CDA as follows:

In passing section 230, Congress sought to spare interactive computer services this grim choice by allowing them to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn't edit or delete. In other words, Congress sought to immunize the removal of user-generated content, not the creation of content:

> [S]ection [230] provides 'Good Samaritan' protections from civil liability for providers . . . of an interactive computer service for ***936** actions to restrict . . . access to objectionable online material. One of the specific purposes of this section is to overrule Stratton-Oakmont [sic] v. Prodigy and any other similar decisions which have treated such providers . . . as publishers or speakers of content that is not their own because they have restricted access to objectionable material. [FN350]

The CDA impacts Internet privacy and security issues in two ways. First, it can impact the liability of an ISP related to postings of information and statements regarding other persons or entities. Second, given its restrictions upon liability, as well as the anonymous status of many posters on blogs, chat rooms or bulletin boards, many companies or individuals that are defamed or otherwise harmed will typically sue the anonymous posters and subpoena their identity from the ISP.

The CDA is also frequently addressed in spyware and phishing cases where software companies gather information and block programs. [FN351] Indeed, a software company that gathered a list of sites that appeared to be phishing sites was immune under the CDA because it gathered the information from a third-party. [FN352]

A. Communications Decency Act-Restrictions Upon Liability

In defamation actions one of the key issues is whether a person is a publisher or speaker of information. The CDA provides that neither providers nor users of an interactive computer service [FN353] will be treated as a publisher or speaker of information that is provided by another information content provider, which therefore eliminates liability. [FN354] The CDA also eliminates liability for any provider or user of an interactive computer service related to:

(1) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers ***937** to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(2) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described above. [FN355]

The CDA appears to apply immunity beyond the mere publication of information. Certain courts have held that the CDA also gives immunity for service providers even where they have taken on "a publisher's traditional editorial functions-such as deciding whether to publish, withdraw, postpone or alter content." [FN356] The CDA does not, however, provide immunity for a service provider where the service provider contributes to the content. The First Circuit addressed the scope of CDA immunity and held, as have other Circuit Courts, that the immunity will apply to sites, even where the construction and operation of the site have some influence on the content that is posted. [FN357] Indeed, in one case a website that provided multiple-choice questions and a series of essay questions that shaped the eventual content was found to fall within the CDA's grant of immunity, even for claims of invasion of privacy. [FN358]

One Ohio federal court recently addressed the scope of CDA immunity with state law claims and found that it applied broadly and barred a number of common law claims. [FN359] However, another court recently held that allegations by the FTC that the sale of pretexted phone records violated the FTC Act were not barred by the CDA because these claims did not seek to treat the defendant as a publisher under the CDA. [FN360]

The CDA has also been applied to the online dating service context and the court addressed whether there was immunity for a ***938** website that allegedly sent false dating profiles, and continued to send profiles of members that were no longer part of the website. [FN361]

B. Immunity for the Conduct of Affiliates

Courts have also applied the CDA immunity to service providers that merely provide Internet connections to the web where the ISPs service is used to send e-mails, even where the e-mails are offensive, illegal, or where they are sent by affiliates. [FN362] In Beyond Systems, the plaintiff alleged it received a number of unsolicited and deceptive e-mails regarding certain websites that were allegedly affiliates of the defendants. [FN363] Notably, the content itself was not created by the defendants. [FN364] The court examined the conduct of Rackspace, a defendant that provided hosting and web services, and concluded that, as an "interactive computer service provider," it could not be held liable under Maryland's anti-spam law, due to the CDA. [FN365]

C. Immunity for Conduct of Users

Another issue that courts have addressed is the liability of websites for user-generated content. Roommates.com is a website that attempts to match potential roommates up in an online forum based upon certain preferences. Roommates.com did two key things as part of the registration process to use its site, in addition to asking general background questions: (1) it provided a structure through a series of mandatory questions regarding sex, sexual orientation, and whether they will bring children; and (2) provided an open-ended "Additional Comments" section. [FN366] A variety of Fair Housing Councils in California brought a lawsuit seeking to hold Roommates.com liable for asking these questions and thereby inducing its users to violate Fair Housing laws. [FN367] Roommates.com believed it was immune from liability due to the CDA because it did not create the content, but instead only displayed the responses of its users. [FN368]

***939** The Roommates.com case addressed an important issue-what is the level of online conduct by a website owner that will defeat immunity. While there have been other cases that have indirectly addressed the issue, Roommates.com is the first case to directly confront this issue. The issue was raised in this case because, as noted above, unlike message boards, blogs, or other forms of online communication, Roommates.com asked questions regarding sex, sexual orientation, and whether the person has children as part of the sign up process. [FN369] According to the plaintiffs, these questions, if asked offline, allegedly violated Fair Housing laws. Additionally, Roommates.com also had a search engine that permitted users to search for potential roommates based upon allegedly discriminatory categories. [FN370]

The Ninth Circuit concluded that the CDA did not provide immunity for certain portions of the Roommates.com website. [FN371] Regarding the mandatory posted questions, the Ninth Circuit concluded that Roommates.com did not have immunity under the CDA. [FN372]

Roommates.com created the questions and choice of answers, and designed its website registration process around them. Therefore, Roommates.com is undoubtedly the "information content provider" as to the questions and can claim no immunity for posting them on its website, or for forcing subscribers to answer them as a condition of using its services.

The CDA does not grant immunity for inducing third parties to express illegal preferences. Roommates.com's own acts-posting the questionnaire and requiring answers to it-are entirely its own doing and thus section 230 of the CDA does not apply to them. Roommates.com is entitled to no immunity. [FN373]

***940** This was because, by posting the mandatory questionnaire, Roommates.com helped develop, at least in part, the content. [FN374] The Ninth Circuit also addressed whether Roommates.com had immunity for the allegedly discriminatory comments made by users in the "Additional Comments" section. The court concluded that Roommates.com had immunity for these statements since it, unlike in the other portions of the site, did not "develop" the content. [FN375]

The Ninth Circuit then addressed the search engine and email notification system created by Roommates.com that permitted users to search for roommates based upon allegedly discriminatory categories. This search engine was not a generic search engine that could be used to search upon discriminatory categories, but rather one that was explicitly based upon allegedly discriminatory categories. [FN376]

Roommates.com's search function is similarly designed to steer users based on discriminatory criteria. [FN377] Roommates.com's search engine thus differs materially from generic search engines such as Google, Yahoo! and MSN Live Search, in that Roommates.com designed its system to use allegedly unlawful criteria so as to limit the results of each search, and to force users to participate in its discriminatory process. [FN378]

The Ninth Circuit also concluded that immunity under the CDA did not exist for placing the same allegedly discriminatory categories in search fields in a search engine. [FN379]

Two other prior Ninth Circuit decisions were then discussed and clarified by the court. The conclusion that minor editorial changes under Batzel were subject to immunity was affirmed, though the court, without directly addressing the issue, appeared to question ***941** whether the editor in that case actually fell within the CDA. [FN380] The court also recognized the distinction between choosing what material is placed in an online posting from an editorial perspective versus making the choice to publish material online in the first place; while the former falls within CDA immunity, the latter does not. [FN381]

The court also clarified its holding in Carafano v. Metrosplash.com. Inc., limiting its prior conclusion: "We correctly held that the website was immune, but incorrectly suggested that it could never be liable because 'no [dating] profile has any content until a user actively creates it.'" [FN382] Going further in a footnote, the court stated "We disavow any suggestion that Carafano holds an information content provider automatically immune so long as the content originated with another information content provider." [FN383] Instead, the court concluded that Carafano was correctly decided because the content at issue was created and developed entirely by the user, using neutral tools without prompting for help from the website operator. [FN384]

D. The CDA and Social Networking

Social networking is a large part of web activity and one issue that has arisen is the scope of CDA immunity in situations where the service provider has played a role as an intermediary for improper conduct, including issues with minors and other forms of alleged sexual misconduct. Certain plaintiffs have alleged that social networking sites know sexual predators are using their services and ***942** therefore CDA immunity does not exist. [FN385] This argument was recently rejected by the Fifth Circuit when it found that MySpace was immune from claims that it had allegedly failed to implement safety procedures to prevent sexual predators from allegedly misusing MySpace. [FN386] The court did not consider the plaintiffs' argument that MySpace lacked immunity under the CDA due to its alleged role in creating the content due to an online questionnaire. However, it should be noted that the Ninth Circuit recently addressed this issue in Roommates.com, [FN387] and given the questionnaire as described in the Doe v. MySpace, Inc. case, it would appear to fall within the "neutral" category that would still support immunity.

E. Communications Decency Act-Immunity v. Defense

While certain courts have referred to the CDA as providing immunity, other courts have characterized the CDA's protections as not immunity from suit, but rather a defense to liability. [FN388]

F. Communications Decency Act-Disclosures by Interactive Computer Services

Providers of interactive computer services must, at the time of entering an agreement with a customer, notify the customer in an appropriate manner that parental control protections are commercially available and these protections may assist in limiting access to material that is harmful to minors. [FN389] The notice must identify, or provide the customer with access to information identifying, current providers of such protections. [FN390]

VIII. Class Action Issues in Privacy Litigation

Class actions are a form of a lawsuit where a large group of people, with similar claims, collectively litigate their claims in court through a class representative that acts on their behalf. This type of action is becoming more and more common in the privacy litigation realm and a discussion of class action issues is included in the ***943** following sections. Generally, in order to state a class action claim in federal court, the plaintiff must comply with Rule 23(a) and this includes showing: voluminous numbers of the parties; commonality of legal and factual issues; typicality of claims and defenses of the class represented; and adequacy of representation. [FN391] In addition to these pre-requisites, a plaintiff must also show that the proposed class of action fits within one or more of the categories of class actions described in Rule 23(b). [FN392]

A. General Issues with Privacy Class Actions

One of the common issues in privacy litigation that defendants address is the typicality requirement. In most cases typicality "refers to the nature of the claim or defense of class representative, not to the specific facts from which it arose or the relief sought." [FN393] Another common issue that is raised by defendants is that the represented parties do not have common interests with the class or that they are unable to prosecute the action vigorously through qualified counsel. [FN394]

B. Class Actions in Federal Court-The Requirements of Rule 23

Class actions are not automatically permitted to proceed in court. They must first be certified by the court and satisfy four threshold requirements:

(1) the class is so numerous that joinder of all members is impracticable;

(2) there are questions of law or fact common to the class;

(3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and

(4) the representative parties will fairly and adequately protect the interests of the class. [FN395]

Essentially, class actions involve the joinder of many people to the action, most of which will not actually participate in the process. On the joinder issue, a party need not show that joinder is impossible, ***944** just impracticable. [FN396] Moreover, while the number of plaintiffs is the main focus of numerosity, it need not be millions of plaintiffs to qualify as a class action. Although a class of one million members easily satisfies the numerosity requirement, some courts have found that a number could be as a low as 40. [FN397]

Rule 23(a)'s commonality requirement "is met if plaintiffs' grievances share a common question of law or of fact." [FN398] This requirement "is usually a minimal burden for a party to shoulder" [FN399] because it does not require identical issues, but rather just that the plaintiff identify "some unifying thread among the members' claims that warrants class treatment." [FN400] However, the common issues must be expressed with some degree of particularity and specificity. [FN401] At some level, courts merge the commonality and typicality requirements. [FN402] This issue was addressed regarding the disclosure of ***945** personally identifiable information in the Parker case and this court found it sufficient that the legal theory and factual question were the same-whether the class members were injured by the disclosure of their personally identifiable information without

notice. [FN403]

Likewise, typicality does not require that "the factual background of each named plaintiff's claim be identical to that of all class members; rather, it requires that the disputed issue of law or fact 'occupy essentially the same degree of centrality to the named plaintiff's claim as to that of other members of the proposed class."' [FN404] In order to satisfy this requirement, "the plaintiffs must show that their interests are aligned with the interests of their fellow class members in order to ensure that each claim will be prosecuted with diligence and care." [FN405] Typicality does not require that the representative plaintiffs' claims be factually identical to all other class members; "[n]evertheless, [their] claims must still share 'the same essential characteristics as the claims of the class at large."' [FN406]

The "adequacy of representation" prong is met if the named plaintiffs "have typical claims, have no interests antagonistic to class members, and be required to make the same showing as the absent class members to establish defendants' liability." [FN407] It should be noted that there is "no simple test for determining if a class will be adequately represented by a named plaintiff" and "each case must be approached on an individualized basis." [FN408] The factors include "'the representative's understanding and involvement in the lawsuit,' 'the willingness to pursue the litigation,' and 'any conflict between the representative and the class."' [FN409]

***946** The party seeking certification bears the burden of establishing these requirements. [FN410] Courts will examine these issues closely, though some of these elements tend to merge. [FN411] However, the class certification procedure itself should not typically devolve into a mini-trial on the merits of the individual or class claims. [FN412]

Additionally, courts previously implied the requirement that the class be definite in order to be certified. [FN413] While this is not a prerequisite for certification under 23(a), amendments to Rule 23(c)(1)(B) now explicitly require that the order certifying the class "must define the class and the class claims, issues, or defenses and this is interpreted as codifying the prior implicit requirements."

If Rule 23(a) is not met then the court must dismiss the class allegations, though it can permit the individual action to proceed. [FN414]

C. Rule 23(b)-A General Overview

If the prerequisites of Rule 23(a) are met, the proposed class must additionally satisfy one of the 3 provisions for certification under Rule 23(b). [FN415] Rule 23(b) permits two forms of class actions-mandatory and "opt-out" class actions. Mandatory class actions-those under 23(b)(1)-(2) focus on classes with similar interests and, as a result, do not require the court to give notice and a chance to opt-out ***947** of the class. [FN416] Class actions brought under 23(b)(3) are opt-out class actions and these require each class member to receive notice, and the opportunity to opt-out of the class. [FN417] Opt-out rights and notice provisions are especially important in the class context because the rights of individual class members will be affected without their actual participation.

The first of the options to meet the requirements of 23(b) is that prosecuting separate actions by or against individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for the party opposing the class, or adjudications with respect to individual class members that, as a practical matter, would be dispositive of the in-

terests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests. [FN418]

The second is that the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole. [FN419] Under Rule 23(b)(2), the class action can contain claims for monetary damages as long as they are not "predominantly" sought and instead are "secondary to the primary claim for injunctive or declaratory relief." [FN420] This typically requires a review of the specific facts and circumstances of each case, including the intent of the plaintiff in brining the suit. [FN421]

Under Rule 23(b)(3) a class action is available where there are common questions of law or fact that "predominate" over any questions affecting only individual members and the class action device is "superior" to other available methods for fairly and efficiently adjudicating the controversy. [FN422] This tests whether the classes are "sufficiently" cohesive to justify adjudication by class representation. [FN423] The matters relevant to this finding include: the class members' interests in individually controlling the prosecution or ***948** defense of separate actions; the extent and nature of any litigation concerning the controversy already begun by or against class members; the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and the likely difficulties in managing a class action. [FN424]

The third is that the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy. [FN425]

1. Examination of 23(b)(1)

The focus of a court's examination of a class action that qualifies under 23(b)(1) is two-fold. For cases under 23(b)(1)(A), the focus is on whether there is a risk that the defendant would be subject to incompatible standards or judgments. This section "takes in cases where the party is obliged by law to treat the members of the class alike (a utility acting toward customers; a government imposing a tax), or where the party must treat all alike as a matter of practical necessity (a riparian owner using water as against downriver owners)." [FN426] In class actions brought under Rule 23(b)(1) one of the factors courts consider is whether compensatory relief is the only relief sought. This is because a class action under Rule 23(b)(1)(A) is not proper if purely monetary, and no declaratory or equitable, relief is sought because the concern over incompatible standards is not present. [FN427]

For cases under 23(b)(1)(B), the court examines whether adjudications with respect to individual class members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications, would substantially impair or impede their ability to protect their interests. [FN428] This typically occurs in "'limited fund' cases, instances in which ***949** numerous persons make claims against a fund insufficient to satisfy all claims." [FN429]

2. Examination of 23(b)(2)

When determining if 23(b)(2) is met, the court must examine whether injunctive relief is the predominant remedy sought by the plaintiffs. Said differently, Rule 23(b)(2) "does not extend to cases in which the appropriate final relief relates exclusively or predominantly to money damages." [FN430] In the Second Circuit, the test used to determine whether money damages are the predominant relief sought, and therefore preclude class certification, is a so-called "ad hoc" test that is based upon a valuation of the relief sought. [FN431] The test states

that a district court:

> [M]ay allow (b)(2) certification if it finds in its informed, sound judicial discretion that (1) the positive weight or value to the plaintiffs of the injunctive or declaratory relief sought is predominant even though compensatory or punitive damages are also claimed, and (2) class treatment would be efficient and manageable, thereby achieving an appreciable measure of judicial economy. [FN432]

In determining whether injunctive or declaratory relief predominates, the court must look at two factors and determine:

> (1) even in the absence of a possible monetary recovery, reasonable plaintiffs would bring the suit to obtain the injunctive or declaratory relief sought; and (2) the injunctive or declaratory relief sought would be both reasonably necessary and appropriate were the plaintiffs to succeed on the merits. Insignificant or sham requests for injunctive relief should not provide cover for (b)(2) certification of claims that are brought essentially for monetary recovery. [FN433]

Applying this to the Parker case (one that sought relief for alleged violation of the Cable Communications Policy Act), the court ***950** concluded that injunctive relief was incidental to the damage claims and therefore this element of Rule 23(b) was not met. [FN434]

3. Examination of 23(b)(3)

Examination under Rule 23(b) involves an analysis of whether the "proposed classes are sufficiently cohesive to warrant adjudication by representation." [FN435] The Second Circuit has found that "[c]lass-wide issues predominate if resolution of some of the legal or factual questions that qualify each class member's case as a genuine controversy can be achieved through generalized proof, and if these particular issues are more substantial than the issues subject only to individualized proof." [FN436] As a result, the predominance inquiry is somewhat related to the commonality and typicality requirement of Rule 23(a), but it is typically seen as a stronger requirement. [FN437]

The Supreme Court has held that Rule 23(b)(3)'s predominance requirement was not met when the purported class members had all been exposed to asbestos products supplied by the defendants, where the class members "were exposed to different asbestos-containing products, for different amounts of time, in different ways, and over different periods." [FN438] The court in PayPal, concluded that the predominance requirement was not met merely because the class members accepted PayPal's user agreement, when in that case, only a small number of claims had become claims for actual damages where there were not common factual and legal issues. [FN439]

4. Notice under Rule 23(b)(3)

Because of procedural differences in classes under Rule 23(b)(2) and 23(b)(3), Rule 23(b)(3) classes can result in the waiver of potential claims or defenses, due process concerns require that putative class members receive notice that their claims are being ***951** adjudicated, or the class may not have res judicata effect. [FN440] The notice requirements are read strictly to require the "best notice practicable" to the names and addresses that could be obtained through reasonable means. [FN441]

D. Potential Defenses Based Upon Individual Reliance

One of the issues faced in privacy litigation, particularly claims that rely upon individual statements to con-

sumers, is individual reliance. If the claim involves proving what each individual knew or relied upon, such as in litigation related to reliance upon a privacy policy, class claims may fail because they do not meet the predominance requirement of Rule 23(b)(3). [FN442]

E. Examples of Class Actions Involving Privacy Concerns

In Parker v. Time Warner Entertainment Company, L.P., the court examined whether a class action was appropriate where the case alleged violation of the Cable Communications Policy Act of 1984. [FN443] In Parker, the plaintiffs alleged that the defendants violated this law by disclosing and selling personally identifiable information about their subscribers to third parties and by failing to provide subscribers with clear and conspicuous notice of its disclosure of such information. [FN444] Specifically, Time Warner was alleged to have collected "detailed" personal information about and from subscribers and sold this information to third parties, including telemarketers, direct marketing services companies, and other Time Warner affiliates and divisions. [FN445] The case also alleged that Time Warner did not comply with the notice requirements of this Act. [FN446] This case was a class action in which the parties sought to settle the case via a proposed settlement that included class certification, and the court rejected the proposal because it did not meet the requirements of Rule ***952** 23 in addition to grounds that damage claims predominated and that notice was not appropriate. [FN447]

F. California Class Action Issues

Most states have developed their own standards for determining whether class actions are appropriate. [FN448] In California, class certification is a procedural tool that may be used only where the common questions of fact or law predominate over those particular to individual plaintiffs. As a conceptual starting point, it should be noted that,

> each member must not be required to individually litigate numerous and substantial questions to determine his right to recover following the class judgment; and the issues which may be jointly tried, when compared with those requiring separate adjudication, must be sufficiently numerous and substantial to make the class action advantageous to the judicial process and to the litigants. [FN449]

But "a class action cannot be maintained where each member's right to recover depends on facts peculiar to his case." [FN450]

California has codified its requirements in Code of Civil Procedure § 382. [FN451] California courts have held that before a class ***953** action can be maintained under Section 382, the plaintiff must first show two basic elements: (1) the existence of an ascertainable class, and (2) a well-defined community of interest among the class members. [FN452]

1. Ascertainable class

The first element under Section 382 is ascertainment of the class. A class is ascertainable if it identifies a group of unnamed plaintiffs by describing a set of common characteristics sufficient to allow members of that group to identify themselves as having a right to recover based on the description. [FN453] This requires an objective definition of the persons in the class-that is, who they are, and how, if notice is required, they can be told about the case and their interest in it. Ascertainability is further determined by examining the size of the class and the means available for identifying class members. [FN454] In other words, can the alleged class be located

with reasonable efficiency, i.e. without unreasonable expense or delay? [FN455] In examining these issues, courts have had to consider whether the class can be determined by the defendants' records. [FN456] In other cases, class actions have failed because the class can only be identified by individuals self-identifying. [FN457]

2. Community of interest

The community of interest requirement is based upon three factors: (a) predominant common questions of law or fact, (b) class representatives with claims or defenses typical of the class, and (c) class representatives who can adequately represent the class. [FN458]

***954** 3. Predominant questions of law or fact

This element generally examines whether "[c]ommon issues would be the principal issues in any individual action, both in terms of time to be expended in their proof and of their importance." [FN459] Class certification is inappropriate in cases where liability and damages are highly individual in nature. [FN460] As an example, this element was satisfied in one matter where a plaintiff alleged that thousands of deeds of trust contained identical impound account provisions that were entered into between a bank and its customers who applied for real estate loans. In this case, the plaintiffs showed that the preprinted form contracts containing the challenged impound account provisions constituted contracts of adhesion. [FN461]

While individual damages can cause denial of class certification, some courts have held that mere differences in computing damages is not sufficient to deny class certification. [FN462] However, differences regarding whether damages exist, or the manner in which they are incurred, are appropriate considerations. [FN463] In one case, the court found that although determination of the alleged unconscionability of what was clearly a contract of adhesion was common to the class, individual differences relating to damages went beyond mere problems of calculation, but rather involved differences as to each individual class member's entitlement to damages. [FN464]

4. Typicality

This factor generally examines whether the class representatives' claims arise from the same nucleus of operative facts as those of other class members. California courts have held this requirement does not necessitate that the interests of the class representatives be identical with those of the class. [FN465] Rather, the requirement is that the class ***955** representatives be situated similarly to the class's other members. [FN466] In showing typicality, the fundamental requirement is that the plaintiff seeking to represent the class actually be a member of the class. [FN467]

An example of a case where class certification was denied due to this issue is Caro. [FN468] In Caro, the plaintiff asserted claims for fraud, violation of a number of statutes, including Business & Professions Code Section 17200, and violation of the CLRA, based on allegations that the class members-buyers of the orange juice-" were deceived by the product's labeling and advertising into believing they were buying 'fresh' orange juice." [FN469] The Court of Appeal held that the representative plaintiff's claims were atypical of the class because at deposition he contradicted the allegations made in the complaint by stating that he had not believed that the orange juice products were fresh and also stated that he did not read the entirety of the orange juice labels. [FN470]

5. Adequate representation

In order to be deemed an adequate class representative, the class action proponent must show she has claims or defenses that are typical of the class, and that she can adequately represent the class. [FN471] This element requires a showing that the class representatives can adequately represent the class, and is related to the typicality requirement discussed above. Generally, the adequacy analysis examines whether the class representative's claims are free of irreconcilable conflicts. [FN472] The key element in determining the class ***956** representative's adequacy is that person's ability and willingness to pursue the class members' claims vigorously. [FN473] This element also examines the competency of counsel. [FN474]

6. Additional showing-substantial benefit to the court and litigants

In addition to the above, the proponent of class certification must also show substantial benefit to the court and litigants, and this generally contemplates a balancing test to determine whether the benefit to litigants and the court is sufficient to justify class action. [FN475]

7. No consideration of the merits

As in federal court, California courts typically do not consider the merits of the case when ruling upon class certification. [FN476] However, where issues affecting the merits of a case are enmeshed with class action requirements, such as whether substantially similar questions are common to the class and predominate over individual questions, a court is authorized to scrutinize a proposed class cause of action to determine whether it is suitable for resolution on a class-wide basis. [FN477]

8. Application to privacy litigation

There have been a number of privacy litigation matters brought as class actions in California, and one of the most common is for violation of Civil Code § 1747.08 [FN478]. The court in Linder v. Thrifty Oil, [FN479] examined the elements of a class action in this context and it provides a good example of certain issues. In Linder, the plaintiff moved to certify the case as a class action with two plaintiff classes. [FN480] The first class was called the “the surcharge class,” and it consisted of more than a million California residents who were allegedly compelled to pay an illegal surcharge of roughly 4 cents per ***957** gallon more than customers paying in cash. [FN481] The second class, called “the penalty class,” was comprised of individuals who used their credit cards to make purchases at service stations that allegedly violated the law by using credit card forms with a preprinted space for cardholders to fill in their telephone numbers. [FN482]

In examining the class certification issues, the trial court denied class certification, partly on the basis that class members would not receive substantial benefit due to the costs and potential recovery-a conclusion that was rejected by the court because it did not share the conclusion that notice by first class mail was required in this case. [FN483] It also rejected this conclusion because it noted that

> [I]t is firmly established that the benefits of certification are not measured by reference to individual recoveries alone. Not only do class actions offer consumers a means of recovery for modest individual damages, but such actions often produce “several salutary by-products, including a therapeutic effect upon those sellers who indulge in fraudulent practices, aid to legitimate business enterprises by curtailing illegitimate competition, and avoidance to the judicial process of the burden of multiple litigation involving identical claims.” [FN484]

Thus, the amount of potential recovery, while significant, was not the only factor to consider, which resulted in the denial of class certification being reversed. [FN485]

***958** G. TCPA Claims and Class Certification

There is a split among courts regarding whether a TCPA claim can be brought as a class action. [FN486] However, even in the courts that permit class actions, [FN487] plaintiffs have faced issues proving that a permissible class exists regarding a number of the requirements, including numerocity, [FN488] commonality, [FN489] typicality, [FN490] as well as the higher burdens of 23(b)(3) because "these cases require an examination of a series of individual transmissions under individual circumstances." [FN491] Other courts have rejected these findings regarding class certification of TCPA claims and permitted classes to be certified. [FN492]

H. Pleading

The damage issues faced in privacy ligation also impact class certification. [FN493]

IX. Class Action Discovery

The California Supreme Court has addressed the permissible scope of class action discovery in Pioneer Electronics (USA), Inc., v. Superior Court. [FN494] The Court of Appeal had ruled that a class action plaintiff could not obtain the names and contact information of other potential plaintiffs, who had also allegedly complained about the product at issue in the case, without a letter being sent to the potential ***959** plaintiffs and the individuals affirmatively consenting to the disclosure. [FN495] The Supreme Court reviewed this decision and ultimately reversed the Court of Appeal. The court first noted the general formulation of invasion of privacy claims in California, as expressed by Hill, which is that the claimant must possess a "legally protected privacy interest," there must be a reasonable expectation of privacy under the particular circumstances, including "customs, practices and physical settings surrounding particular activities," and the invasion of privacy must be "serious" in nature and the actual or potential impact must be an "egregious" breach of social norms. [FN496] The Court of Appeal had required Colonial Life notices to the other potential plaintiffs and required the letter to seek affirmative consent before disclosure could occur, rather than giving the individual the option to "opt-out" and have disclosure occur if there was silence. [FN497] Here, the Supreme Court concluded that there was a somewhat reduced expectation of privacy due to the fact that the consumers at issue were ones that had complained and that disclosure of contact information, particularly with a right to opt-out, was not a serious invasion of privacy. [FN498] It also noted that some consumers might actually prefer that their information be disclosed in this context. Thus, it concluded that a letter that informed the consumers of their right to object, with an opt-out right, was sufficient. [FN499]

In a recent case, the Court of Appeal addressed the scope of class action discovery where the members of the class had executed forms that purportedly impacted their expectation of privacy. [FN500] In this case the class arose from an alleged violation of California labor laws. [FN501] The defendant employer had its current employees execute a form that gave them a choice regarding whether they desired to have their information disclosed to third parties, including in the class action context. [FN502] The defendant argued that as a result of most employees ***960** choosing not to disclose, an "opt-in" class notice should be used. [FN503] The court examined its recent decision in Puerto v. Superior Court, [FN504] which examined a similar issue, albeit without the form in question. The court noted that in its prior ruling that while discovery is quite broad:

> [It] "is not absolute, particularly where issues of privacy are involved. The right of privacy in the California Constitution (art. I, § 1), 'protects the individual's reasonable expectation of privacy against a

serious invasion."' The court must balance the public need against the weight of the privacy right. This "requires a careful evaluation of the privacy right asserted, the magnitude of the imposition on that right, and the interests militating for and against any intrusion on privacy." In conducting this evaluation, we must determine whether the person claiming the privacy right has a "'legally protected privacy interest"'; whether the person has a "reasonable expectation of privacy under the particular circumstances, including the customs, practices, and physical settings surrounding particular activities"; and whether the invasion of privacy is serious rather than trivial. [FN505] Despite this, in Puerto, the court permitted the discovery, finding:

> [T]he requested information, while personal, [was] not particularly sensitive, as it [was] merely contact information, not medical or financial details, political affiliations, sexual relationships, or personal information. The employees had been identified by Wild Oats as witnesses; contact information for witnesses ordinarily is produced during discovery, and "it is neither unduly personal nor overly intrusive. We concluded that there was 'no evidence that disclosure of the contact information for these already identified witnesses [was] a transgression of the witnesses' privacy that [was] sufficiently serious in [its] nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right."' [FN506]

Ultimately the court examined the form at issue in the case and was not convinced that the form impacted the employees' expectation of privacy, particularly in connection with what it considered to be a waiver of class action notice. [FN507]

***961** The California Court of Appeal examined these issues in Alch v. Superior Court. [FN508] In this case, television writers filed class-action lawsuits against a number of different defendants alleging industry-wide practice of age discrimination. [FN509] As part of the discovery process, privacy notices were sent to 47,000 Writers Guild members advising the members of their right to object to the disclosure of their information based upon privacy concerns. [FN510] Information was sought to try to provide input for statistical analysis as well as the representation practices of employers and talent agencies. [FN511] The initial subpoena sought sensitive information as well as non-sensitive information, but the subpoenas were later modified over time. [FN512] The prior requests included requests for social security numbers, but these were later redacted as part of the protective order in place in the case. [FN513]

The court began the examination of the issue by reviewing the Pioneer Electronics case, as well as the Hill case. The court noted that in order to assess whether a discovery order that implicated privacy rights was proper, the court must first look at whether the privacy claimant possesses a legally protected privacy interest. [FN514] Typically there are two general types of privacy under this analysis: autonomy privacy, which was identified as the interest in making intimate personal decisions or conducting personal activities without observation, intrusion or interference, as well as informational privacy, which is the interest "in precluding the dissemination or misuse of sensitive or confidential information." [FN515] The privacy claimant must also have a reasonable expectation of privacy under the specific circumstances, including the "customs, practices and physical settings surrounding a particular activities [which] may create or inhibit reasonable expectations of privacy." [FN516] Third, to be actionable, invasions of privacy "must be sufficiently serious in their nature, scope and actual or potential impact to constitute an egregious breach ***962** of the social norms of the underlying privacy right." [FN517] Finally, the court noted that if these three criteria were met then the privacy interest must "be measured against other competing or countervailing interests in a 'balancing' test." [FN518]

Ultimately, the court concluded that the criteria for invasion of privacy were established and that this invasion was serious, but that the writers in the case had demonstrated the information was "directly" relevant to

their claims and “essential to the fair resolution” of their lawsuit. [FN519] The court did note, however, that information sought in this case was not confidential information that is the type of sensitive information typically found in personnel files, and therefore distinguished the cases. [FN520]

Ultimately, in completing its analysis of this issue, the court noted that the demographic data sought by plaintiffs in this case, which included name, date of birth, date of death, gender, race, and residential zip code, was not “sensitive” information. [FN521]

One issue that arose in connection with a claim for an alleged violation of Penal Code § 632 is whether the named plaintiffs in a proposed class action could seek discovery from the defendant of the names of potential class members who were allegedly illegally wiretapped. [FN522] In this case, the defendant only provided the account number and not names or contact information. [FN523] The defendant argued that to permit the discovery would permit the plaintiffs to abuse the discovery process because they did not have standing to file the case in the first instance. [FN524] The court disagreed, finding that it ***963** was proper in this case to permit precertification discovery and an amendment of the pleading. [FN525]

X. Conclusion

Privacy litigation presents some of the most high-stakes litigation in an arena where the bases of the claims are often opaque. Given the ever-increasing value of information, coupled with increasing public concern, privacy litigation is here to stay and will only increase in the future as both consumers and businesses take steps to protect their most sensitive information.

[FNd1]. Andrew **Serwin** is the founding chair of the Privacy Security and Information Management Practice and a partner at Foley & Lardner LLP specializing in information management matters. He has extensive experience in assisting companies with privacy and security issues, including state, federal, and international restrictions on the use and transfer of information, security breach compliance, incident response, information management litigation, marketing restrictions, and the drafting and implementation of privacy and security policies, as well as broad experience in technology and business law, including corporate finance, partnership law, securities, e-commerce, software development and licensing, and intellectual property licensing and protection. He is the author of Information Security and Privacy: A Practical Guide to Federal, State and International Law (2nd ed. West 2008), a 3,600 page treatise on information security and privacy, and the Internet Marketing Law Handbook, both published by Thomson-West, as well as Privacy 3.0: The Principle of Proportionality, which will be published this year by the University of Michigan Journal of Law Reform. He has written over seventy articles, predominantly on information management and Internet issues, is the author of the advertising section of the ABA Model Web Site: A Knowledge Management Approach to E-Business that provides guidance on best practices for Internet issues, and is the Co-Chair and principle author of the Privacy and Security Section of the ABA's publication, Selling Products and Services and Licensing Software Online: An Interactive Guide With Legal Forms and Commentary to Privacy, Security and Consumer Law Issues (June 2007). He also serves on the privacy and legal subcommittees of the Privacy & Security Advisory Board of the California Health and Human Services Agency by the California Office of HIPAA Implementation, the Publications Board of the American Bar Association's Business Law Section, and the editorial board of the Cyberspace Lawyer and the Privacy and Information Law Report. He is also the former Co-Chair of the California State Bar's Cyberspace Law Committee.

[FN1]. See Kearney v. Salomon Smith Barney, Inc., 137 P.3d 914 (Cal. 2006).

[FN2]. See Restatement (Second) of Torts §§ 652B-652E (1977).

[FN3]. See id. § 652B cmt. a.

[FN4]. See id. § 652B.

[FN5]. See id. § 652C.

[FN6]. See id. § 652C cmt. a.

[FN7]. See id. § 652D.

[FN8]. See id. § 652D cmt. a.

[FN9]. See id. § 652E.

[FN10]. Kearney v. Salomon Smith Barney, Inc., 137 P.3d 914 (Cal. 2006).

[FN11]. 18 U.S.C. § 1030 (2006).

[FN12]. Id. §§ 2510-2522. (2006).

[FN13]. 15 U.S.C. §§ 7701-7713 (2006).

[FN14]. For a more detailed discussion of these laws, please see Andrew **Serwin**, Information Security and Privacy: A Practical Guide to Federal, State, and International Law 102-103 (2nd ed. West 2008).

[FN15]. 18 U.S.C. §§ 1030(a)(2)(C)-(a)(3) (2006).

[FN16]. See id. § 1030(a)(4); see also Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450-51 (E.D. Va. 1998); YourNetDating, Inc. v. Mitchell, 88 F. Supp. 2d 870, 872 (N.D. Ill. 2000).

[FN17]. 18 U.S.C. § 1030(a)(5)(A)(i)-(iii) (2006).

[FN18]. See id. § 1030(a)(5)(B)(i)-(v).

[FN19]. Theofel v. Farey-Jones, 359 F.3d 1066, 1078 (9th Cir. 2004).

[FN20]. Id.

[FN21]. United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000).

[FN22]. Id.

[FN23]. Garland-Sash v. Lewis, No. 05 Civ. 6827(WHP), 2007 WL 935013, at *2-3 (S.D.N.Y. Mar. 26, 2007) (citing In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524 n.33 (S.D.N.Y. 2001)); Letscher v. Swiss Bank Corp., No. 94 Civ. 8277(LBS), 1996 WL 183019, at *3 (S.D.N.Y. Apr. 16, 1996).

[FN24]. Successfactors, Inc. v. Softscape, Inc., 544 F. Supp. 2d 975, 981 (N.D. Cal. 2008) (“In such cases courts

have considered the cost of discovering the identity of the offender or the method by which the offender accessed the protected information to be part of the loss for the purpose of the CFAA.") (citing Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 963-64 (D. Ariz. 2008)); cf. Tyco Int'l (US), Inc. v. John Does, 1-3, No. 01 Civ. 3856 RCCDF, 2003 WL 21638205, at *2 (S.D.N.Y. July 11, 2003).

[FN25]. Middleton, 231 F.3d at 1214.

[FN26]. Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901, at *6 (N.D. Ga. Nov. 7, 2000); see also Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 477-478 (S.D.N.Y. 2004), aff'd, 166 F. App'x 559 (2d Cir. 2006) (holding that lost revenue and remedial costs did not constitute loss under CFAA).

[FN27]. Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 934 (9th Cir. 2004); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001).

[FN28]. Wilson v. Moreau, 440 F. Supp. 2d 81, 110 (D.R.I. 2006).

[FN29]. Spangler, Jennings & Dougherty, P.C. v. Mysliwy, 2:05-cv-00108-JTM-APR (N.D. Ind. Mar. 31, 2006), available at http:// www.steptoe.com/publications/405e.pdf.

[FN30]. Id. at 3.

[FN31]. Id. at 10.

[FN32]. Id. at 3.

[FN33]. Id. at 13; see also Resdev, LLC v. Lot Builders Ass'n, Inc., No. 6:04-CV-137ORL31DAB, 2005 WL 1924743, at *5 n.3 (M.D. Fla. Aug 10, 2005) (noting that damages under CFAA requires some finding of "diminution in the completeness or usability of data or information on a computer system"); Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901, at *6 (N.D. Ga. Nov. 7, 2000) (holding that investigative costs are disallowed as damage under the CFAA where alleged incident did not result in "structural" damage to the network).

[FN34]. P.C. of Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore, L.L.C., No. 04-4554(JAG), 2007 WL 708978, at *3 (D.N.J. Mar. 5, 2007).

[FN35]. Id. at *4.

[FN36]. The court stated, "As the Second Circuit found, 'the plain language of the [CFAA] treats lost revenue as a different concept from incurred costs, and permits recovery of the former only where connected to an 'interruption in service.;"' Nexans Wires S.A. v. Sark-USA, Inc., 166 Fed.Appx. 559, 2006 WL 328292, at *4 (2d Cir. 2006) (citing Civic Ctr. Motors, Ltd. v. Mason Street Imp. Cars, Ltd., 387 F. Supp. 2d 378, 382 (S.D.N.Y. 2005) (ruling that loss of "competitive edge" claim not caused by computer impairment or computer damage was not cognizable under the CFAA); Resdev, LLC v. Lot Builders Ass'n, No. 04-CIV-1374, 2005 WL 1924743, at *5 (M.D. Fla. Aug. 10, 2005) (similar)." Id. at *5.

[FN37]. P.C. of Yonkers, No. 04-4554(JAG), 2007 WL 708978, at *4 (citing 18 U.S.C. § 1030(e)(11) (2006)).

[FN38]. Id.

[FN39]. Id. at *4-6.

[FN40]. Id. at *5.

[FN41]. See Therapeutic Research Faculty v. NBTY, 488 F. Supp. 2d 991 (E.D. Cal. 2007) (citing Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000)) (holding that a claim could be stated under the CFAA against a party that exceeded authorized use of password and thereby obtained additional access to licensed materials); see also PharMerica, Inc. v. Arledge, 2007 WL 865510, at *6-7 (M.D. Fla. Mar. 21, 2007) (holding that an employer had demonstrated likelihood of success on CFAA claim where an employee that downloaded confidential information to use with a competitor and deleted files and records related to the downloading); H & R Block E. Enter., Inc. v. J & M Secs., LLC, 2006 WL 1128744, at *4 (W.D. Mo. Apr. 24, 2006); Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004); Pacific Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003), citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 578 (1st Cir. 2001).

[FN42]. Cenveo Corp. v. CelumSolutions Software GMBH & Co KG, 504 F. Supp. 2d 574, 581 (D. Minn. 2007) (dismissing CFAA claim based upon improper access to an employer's confidential information because the complaint did not allege an interruption of service, and therefore failed to allege loss); see also Spangler, Jennings & Dougherty, P.C. v. Mysilwy, 2:05-cv-00108-JTM-APR, at *12-13 (N.D. Ind. Mar. 21, 2006) (finding that allegations of downloading of firm information by an attorney who was leaving her employer failed to demonstrate a CFAA because there was no allegation of system impairment, and therefore no loss).

[FN43]. EF Cultural Travel, 274 F.3d at 578-79.

[FN44]. Id. at 578.

[FN45]. Id.

[FN46]. Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (“The facts before the Court establish that defendants violated 18 U.S.C. 1030(a)(2)(C) of the Computer Fraud and Abuse Act, which prohibits individuals from ‘intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] information from any protected computer if the conduct involved an interstate or foreign communication.’ Defendants' own admissions satisfy the Act's requirements. Defendants have admitted to maintaining an AOL membership and using that membership to harvest the e-mail addresses of AOL members. Defendants have stated that they acquired these e-mail addresses by using extractor software programs. Defendants' actions violated AOL's Terms of Service, and as such was unauthorized. Plaintiff contends that the addresses of AOL members are ‘information’ within the meaning of the Act because they are proprietary in nature. Plaintiff asserts that as a result of defendants' actions, it suffered damages exceeding $5,000, the statutory threshold requirement.”).

[FN47]. YourNetDating, Inc. v. Mitchell, 88 F. Supp. 2d 870, 870-71 (N.D. Ill. 2000).

[FN48]. Id. at 872.

[FN49]. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 239 (S.D.N.Y. 2000), aff'd as modified, 356 F.3d 393,395 (2d Cir. 2004).

[FN50]. Internet Archive v. Shell, 505 F. Supp. 2d 755, 765 (D. Colo. 2007).

[FN51]. Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435 (N.D. Tex. 2004).

[FN52]. Shaw v. Toshiba Am. Info. Sys., Inc., 91 F. Supp. 2d 926 (E.D. Tex. 1999).

[FN53]. See N. Tex. Preventive Imaging L.L.C. v. Eisenberg, 1996 WL 1359212, at *7 (C.D. Cal. Aug. 19, 1996).

[FN54]. In re Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1277 (C.D. Cal. 2001); In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 523-24 (S.D.N.Y. 2001) (holding that "damages" may be aggregated across all alleged victims, but only for each discrete act and each act must meet the statutory damage requirements).

[FN55]. See, e.g., Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1154 (W.D. Wash. 2001).

[FN56]. In re Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 14-15 (D. Mass. 2002), rev'd, 329 F.3d 9 (1st Cir. 2003).

[FN57]. United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

[FN58]. See, e.g., Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

[FN59]. Id. at 1071.

[FN60]. Id.

[FN61]. Id. at 1078-79.

[FN62]. United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

[FN63]. Id. at 1076.

[FN64]. See, e.g., I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 523 (S.D.N.Y. 2004).

[FN65]. Id. at 526.

[FN66]. See, e.g., Cal. Penal Code § 502(c)(5) (West 2007).

[FN67]. See id. § 502.

[FN68]. See, Va Code Ann. §§ 18.2-152.2- 152.12.

[FN69]. 18 U.S.C. §§ 2510-2522 (2006).

[FN70]. Id.

[FN71]. Id. §§ 2701-2712 (2006).

[FN72]. Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 (2nd Cir. 2005); Organizacion Jd Ltda. v. U.S. Dept. of Justice, 124 F.3d 354, 356 (2d Cir. 1997).

[FN73]. 18 U.S.C. § 2520 (2006); 18 U.S.C. § 2507 (2006).

[FN74]. Id. § 2510(12) (2006) ("Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.").

[FN75]. Id. § 2511(1)(a) (2006).

[FN76]. Id. § 2511(2)(g)(i).

[FN77]. Id. § 2511(2)(a)(i).

[FN78]. Id. § 2511(2)(h)(ii).

[FN79]. Id. § 2511(2)(a)(ii)(A).

[FN80]. Id. § 2511(3)(b)(ii).

[FN81]. Id. § 2511(3)(b)(iii).

[FN82]. Id. § 2511(3)(b)(iv).

[FN83]. Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 459-60 (5th Cir. 1994); United States. v. Moriarty, 962 F. Supp. 217, 221 (D. Mass. 1997) (drawing temporal distinction between acquisition of communications during transmission under Title I and acquisition of contents of communications in a non-contemporaneous manner under Title II).

[FN84]. Bohach v. City of Reno, 932 F. Supp. 1232, 1236-37 (D. Nev. 1996) (holding electronic communications are not intercepted when they are in electronic storage).

[FN85]. Moriarty, 962 F. Supp. at 220-21.

[FN86]. 18 U.S.C. § 2511(2)(g)(i) (2006).

[FN87]. Id. § 2510(4) ("'[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.").

[FN88]. Id. § 2510(2) ("'[O]ral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication....").

[FN89]. Id. § 2510(12)(A)-(D) ("'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include: (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device; or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds....").

[FN90]. Id. § 2510(5)(a)-(b) ("'[E]lectronic, mechanical, or other device' means any device or apparatus which

can be used to intercept a wire, oral, or electronic communication other than (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal....").

[FN91]. Id. § 2510(1) ("'[W]ire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce....").

[FN92]. Id. § 2511(1)(a)-(b) (2006).

[FN93]. Id. § 2510(8) ("'[C]ontents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication....").

[FN94]. Id. § 2511(1)(c).

[FN95]. Id. § 2511(1)(d).

[FN96]. Id. § 2511(1)(e)(iv).

[FN97]. Id. § 2520(a) (2006).

[FN98]. Id. § 2520(b)(1)-(b)(3).

[FN99]. Id. § 2520(a).

[FN100]. Id. § 2520(c)(1).

[FN101]. Id. § 2520(c)(2).

[FN102]. Id. § 2701(a)(1) (6).

[FN103]. Id. § 2701(a)(2).

[FN104]. Id. § 2701(c)(1)- (c)(2).

[FN105]. Id. § 2703(a).

[FN106]. Id. § 2703(b)(2)(A) (noting that the communication can also be created by means of computer processing of communications received by means of electronic transmission).

[FN107]. Id. § 2711(2) ("'[R]emote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system....")

[FN108]. Id. § 2703(b)(2).

[FN109]. Id. §2703(b)(1).

[FN110]. See generally id. § 2706(a).

[FN111]. Id. § 2707(b)(1)-(b)(3).

[FN112]. Id. § 2707(c).

[FN113]. In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001).

[FN114]. Id. at 497.

[FN115]. Id. at 503.

[FN116]. Id.

[FN117]. Id. at 513 (“To summarize, plaintiffs' GET, POST and GIF submissions are excepted from §2701(c)(2) because they are ‘intended for’ the DoubleClick-affiliated Web sites who have authorized DoubleClick's access.”); see also In re Am. Airlines Privacy Litig., 370 F. Supp. 2d 552 (N.D. Tex. 2005).

[FN118]. Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008).

[FN119]. Id. at 896.

[FN120]. Id. at 895-96.

[FN121]. Id.

[FN122]. Id. at 898.

[FN123]. Id.

[FN124]. Id. at 896.

[FN125]. See id. at 896.

[FN126]. Id. at 897.

[FN127]. Id. at 902.

[FN128]. Id. at 900.

[FN129]. Id. at 898-99.

[FN130]. Id. at 900.

[FN131]. Id. at 903.

[FN132]. Id. at 903, 908-09.

[FN133]. Id. at 908-09.

[FN134]. Id. at 906.

[FN135]. Id. at 907-08.

[FN136]. Id. at 907

[FN137]. Id. at 907-08.

[FN138]. Id. at 907.

[FN139]. Id. at 907-08.

[FN140]. Kearney v. Salomon Smith Barney, Inc., 137 P.3d 914 (2006).

[FN141]. Id. at 918.

[FN142]. Cal. Penal Code §632 (1999); Kearney, 137 P.3d at 917, 929-30.

[FN143]. Kearney, 137 P.3d at 917.

[FN144]. Id. at 920.

[FN145]. Id. at 937.

[FN146]. 15 U.S.C. § 7704(a)(1) (2006).

[FN147]. Id. § 7702(2)(a).

[FN148]. Id. § 7702(17)(A).

[FN149]. Aitken v. Commc'n Workers of Am., 496 F. Supp. 2d 653, 666 (E.D. Va. 2007).

[FN150]. 15 U.S.C. § 7706(g)(1) (2006).

[FN151]. See Hypertouch, Inc. v. Kennedy-Western Univ., No. C 04-05203 SI, 2006 WL 648688 at *4 (N.D. Cal. Mar. 8, 2006).

[FN152]. Gordon v. Virtumundo, Inc., No. 06-0204-JCC, 2007 WL 1459395 at *8 (W.D. Wash. May 15, 2007) (noting the divergence in judicial opinions on the issue where the Gordon court required more than the mere inconvenience of receiving spam to satisfy the “adversely affected” requirement under CAN-SPAM).

[FN153]. Id. at *1.

[FN154]. Id. at *2, *7.

[FN155]. Id. at *8.

[FN156]. Id.

[FN157]. ASIS Internet Serv. et al. v. Active Response Group, No. C07 6211 TEH at 2 (N.D. Cal. July 30, 2008) (order denying motion to dismiss).

[FN158]. See, e.g., Haselton et al. v. Quicken Loans, Inc., No. C07-1777RSL at 5-7 (W.D. Wash. Oct. 14, 2008) (order granting motion for partial summary judgment).

[FN159]. Ferguson v. Quinstreet, Inc., No. C07-5378RJB, 2008 WL 3166307 at *5-6 (W.D. Wash. Aug.5, 2008).

[FN160]. Id. at *6 (citing Gordon v. Virtumundo, Inc., No. 06-0204-JCC, 2007 WL 1459395 at *7 (W.D. Wash. May 15, 2007)).

[FN161]. Id. at *2, *6.

[FN162]. Id. at *6.

[FN163]. Id.

[FN164]. Id.

[FN165]. Id.

[FN166]. 15 U.S.C. § 7707(b)(1) (2006).

[FN167]. Omega World Travel, Inc. v. Mummagraphics Inc., 469 F.3d 348, 352 (4th Cir. 2006) (citing Maryland v. Louisiana, 451 U.S. 725, 746 (1981)).

[FN168]. Id. at 352 (citing Medtronic, Inc. v. Lohr, 518 U.S. 470, 485 (1996)).

[FN169]. Id. at 352-353 (citing Medtronic, Inc. v. Lohr, 518 U.S. 470, 486 (1996)).

[FN170]. Id. at 353.

[FN171]. Id. at 353-54.

[FN172]. Wash. Mut. Bank v. Super. Ct., 89 Cal. Rptr.2d 560, 567 (Cal. Ct. App. 1999) (citing Cipollone v. Liggett Group, Inc., 505 U.S. 504, 523 (1992)).

[FN173]. Id. at 567 (citing CSX Transp., Inc. v. Easterwood, 507 U.S. 658, 664 (1993); Cipollone, 505 U.S. at 523).

[FN174]. Maryland v. Louisiana, 451 U.S. 725, 746 (1981).

[FN175]. Viva! Intern. Voice For Animals v. Adidas Promotional Retail Operations, Inc., 162 P.3d 569, 572 (2007).

[FN176]. Id. at 572-73.

[FN177]. Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 373 (2000).

[FN178]. White Buffalo Ventures, LLC v. Univ. of Tex. at Austin, 420 F.3d 366, 368-69 (5th Cir. 2005).

[FN179]. Id. at 368.

[FN180]. Id. at 373-74.

[FN181]. Kleffman v. Vonage Holdings Corp., No. CV 07-2406GAFJWJX, 2007 WL 1518650, at *3 (C.D. Cal. 2007).

[FN182]. 16 C.F.R. § 310 (2008); **Serwin**, supra note 14, at 1258.

[FN183]. § 310.4(7)(b)(iii)(B) (2008); **Serwin**, supra note 14, at 1258.

[FN184]. **Serwin**, supra note 14, at 1269-81.

[FN185]. Id. at 1258.

[FN186]. Id.

[FN187]. Id.

[FN188]. 15 U.S.C. § 6101-08 (2000). This law is also known as the "Telephone Consumer Protection Act," or "TCPA."

[FN189]. 16 C.F.R. § 310.2(bb) (2008) ("'Telemarketer' means any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer or donor.").

[FN190]. Id. § 310.2(z) ("'Seller' means any person who, in connection with a telemarketing transaction, provides, offers to provide, or arranges for others to provide goods or services to the customer in exchange for consideration.").

[FN191]. Id. § 310.2(v) ("'Person' means any individual, group, unincorporated association, limited or general partnership, corporation, or other business entity.").

[FN192]. Id. § 310.2(u) ("'Outbound telephone call' means a telephone call initiated by a telemarketer to induce the purchase of goods or services or to solicit a charitable contribution.").

[FN193]. Id. §310.2(f) ("'Charitable contribution' means any donation or gift of money or any other thing of value.").

[FN194]. Id. § 310.2(n) (establishing business relationship means a relationship between a seller and a consumer based on: (1) the consumer's purchase, rental, or lease of the seller's goods or services or a financial transaction between the consumer and seller, within the eighteen (18) months immediately preceding the date of a telemarketing call; or (2) the consumer's inquiry or application regarding a product or service offered by the seller, within the three (3) months immediately preceding the date of a telemarketing call).

[FN195]. Id. § 310.4(b)(1)(iii)(A) to (B).

[FN196]. Id. § 310.4(b)(1)(iv) ("[A]n outbound telephone call is 'abandoned' under this section if a person an-

swers it and the telemarketer does not connect the call to a sales representative within 2 seconds of the person's completed greeting.")

[FN197]. Id. § 310.4(b)(1)(iv).

[FN198]. Id. § 310.4(b)(2).

[FN199]. Id. § 310.4(b)(v)(A)(i)-(iv).

[FN200]. Id. § 310.4(b)(v)(B)(i)-(ii)(A)(1).

[FN201]. Id. § 310.4(b)(v)(B)(i)-(ii)(A)(2)-(3).

[FN202]. Id. § 310.4(b)(v)(B)(i)-(ii)(B)(1)-(3).

[FN203]. Id. § 310.2(cc). Telemarketing means a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call. The term does not include the solicitation of sales through the mailing of a catalog which: contains a written description or illustration of the goods or services offered for sale; includes the business address of the seller; includes multiple pages of written material or illustrations; and has been issued not less frequently than once a year, when the person making the solicitation does not solicit customers by telephone but only receives calls initiated by customers in response to the catalog and during those calls takes orders only without further solicitation. For purposes of the previous sentence, the term "further solicitation" does not include providing the customer with information about, or attempting to sell, any other item included in the same catalog which prompted the customer's call or in a substantially similar catalog.

[FN204]. Id. § 310.4(b)(3)(i)-(vi).

[FN205]. Id. § 310.4(b)(4).

[FN206]. USA Tax Law Ctr., Inc. v. Office Warehouse Wholesale, LLC, 160 P.3d 428 (Colo. Ct. App. 2007).

[FN207]. See Dun-Rite Constr., Inc. v. Amazing Tickets, Inc., No. 04-3216, 2004 WL 3239533, at *1 (6th Cir. 2004); Murphy v. Lanier, 204 F.3d 911, 912-13 (9th Cir. 2000); Nicholson v. Hooters of Augusta, Inc., 136 F.3d 1287, 1288-89 (11th Cir. 1998); ErieNet, Inc. v. Velocity Net, Inc., 156 F.3d 513, 514 (3d Cir. 1998); Foxhall Realty Law Office, Inc. v. Telecomms. Premium Servs., Ltd., 156 F.3d 432, 434 (2d Cir. 1998); Hirz v. Travelcomm Indus., Inc., No. 1:07 CV 01833, 2007 WL 1959293, at *1-2 (N.D. Ohio 2007) (citing; Ari Weitzner, M.D., P.C. v. Sciton, Inc., No. 05-CV-2533 (SLT)(MDG), 2007 WL 2891521, at *1-2 (E.D.N.Y. 2007) (explaining there is no federal court jurisdiction for TCPA claim); Gratt v. Etourandtravel, Inc., Nos. 06-CV-1965 (FB)(JO), 06-CV-1631(FB)(KAM), 2007 WL 2693903, at *1 (E.D.N.Y. 2007)).

[FN208]. First Capital Mortgage Corp. v. Union Fed. Bank of Ind., 872 N.E.2d 84, 85 (Ill. App. Ct. 2007).

[FN209]. Hirz v. Travelcomm Indus., Inc., No. 1:07 CV 01833, 2007 WL 1959293, at *1-2 (N.D. Ohio 2007).

[FN210]. Cal. Bus. & Prof. Code § 17591 (Deering 2007).

[FN211]. Id. § 17593(a)(1)-(3).

[FN212]. Id. § 17593(b).

[FN213]. Id.

[FN214]. Id.

[FN215]. Id.

[FN216]. Id. § 17593(c).

[FN217]. Id. § 17593(d).

[FN218]. Id. § 17594.

[FN219]. Id. § 17594(a)-(b).

[FN220]. 47 U.S.C. § 227(a)(3) (2006). The term "telephone facsimile machine" means equipment which has the capacity (A) to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or (B) to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper.

[FN221]. Id. § 227(a)(5) ("The term 'unsolicited advertisement' means any material advertising the commercial availability or quality of any property, goods, or services which is transmitted to any person without that person's prior express invitation or permission, in writing or otherwise.").

[FN222]. Id. § 227(a)(2). The term "established business relationship," for purposes only of section 1:16 of this chapter, shall have the meaning given the term in section 64.1200 of title 47, Code of Federal Regulations, as in effect on January 1, 2003, except that-(A) such term shall include a relationship between a person or entity and a business subscriber subject to the same terms applicable under such section to a relationship between a person or entity and a residential subscriber; and (B) an established business relationship shall be subject to any time limitation established pursuant to paragraph (2)(G).

[FN223]. Id. § 227 (c)(ii)(I)-(II).

[FN224]. Id. § 227 (c)(ii)(II).

[FN225]. See id. § 227(c)(iii).

[FN226]. Catalyst Strategic Design, Inc. v. Kaiser Found. Health Plan, Inc., 64 Cal.Rptr.3d 55, 57 (2007).

[FN227]. See Catalyst Strategic Design, Inc. v. Kaiser Foundation Health Plan, Inc., 153 Cal. App. 4th 1328 (2007).

[FN228]. 47 U.S.C. § 227(b)(2)(D)(ii) (2006).

[FN229]. Id.

[FN230]. Id. § 227(b)(2)(D)(iv)(I-II).

[FN231]. Id. § 227(b)(2)(D)(v).

[FN232]. Id. § 227(b)(2)(E)(ii-iii).

[FN233]. Collegenet, Inc. v. XAP Corp., 442 F. Supp. 2d 1070, 1074 (D. Or. 2006).

[FN234]. Collegenet, 442 F. Supp. 2d at 1070.

[FN235]. Id. at 1072.

[FN236]. Id. at 1074.

[FN237]. Id. at 1077.

[FN238]. Id. at 1072.

[FN239]. Id. at 1072-73.

[FN240]. Id. at 1074.

[FN241]. Id. at 1075.

[FN242]. Id. at 1077.

[FN243]. Id.

[FN244]. Id.

[FN245]. Id. at 1079-80.

[FN246]. Cal Bus. & Prof Code § 17200 (Deering 2007).

[FN247]. Id.

[FN248]. Id. § 17203.

[FN249]. Id. § 17204.

[FN250]. Id. § 17204.

[FN251]. Party City Corp. v. Superior Court, 86 Cal. Rptr. 3d 721, 724 (Cal. Ct. App. 2008).

[FN252]. Andrew **Serwin**, Internet Marketing Law Handbook § 2:2 (West 2007).

[FN253]. Id.

[FN254]. Id.

[FN255]. Cal Bus. & Prof Code § 17200 (2007); Kasky v. Nike, Inc., 45 P.3d 243, 249 (2002).

[FN256]. Dean Witter Reynolds, Inc. v. Superior Court, 259 Cal. Rptr. 789, 791 (Cal. Ct. App. 1989).

[FN257]. Stop Youth Addiction, Inc. v. Lucky Stores, Inc., 950 P.2d 1086 (Cal. 1998).

[FN258]. Korea Supply Co. v. Lockheed Martin Corp., 63 P.3d 937 (Cal. 2003).

[FN259]. See Cal. Bus. & Prof. Code §§ 17203, 17535 (Deering 2007).

[FN260]. See generally id. §§ 17500 et seq. (However, the false advertising law (sections 17500, et seq.), which is expressly incorporated into the UCL, provides its own set of civil and criminal remedies.); See also id. §§ 17203 and 17534.5 (These remedies include criminal penalties, injunctive relief, civil penalties, attorneys' fees, and restitution.); People v. Bestline Prods., Inc., 132 Cal.Rptr. 767, 795-96 (1976) (explaining that, as with the remedies available under the UCL, the remedies under the false advertising law are cumulative to other remedies provided by state law).

[FN261]. Cal. Bus. & Prof. Code § 17203 (Deering 2007).

[FN262]. Accord, Cortez v. Purolator Air Filtration Prods. Co., 999 P.2d 706, 709 (2000) (discussing the court's sweeping powers to create appropriate relief).

[FN263]. See, e.g., Comm. on Children's Television, 673 P.2d 660 (1983); People v. Superior Court, 507 P.2d 1400 (1973); Barquis v. Merchs. Collection Assn., 496 P.2d 817 (1972) (granting injunctive relief).

[FN264]. Cal. Bus. & Prof. Code § 17203 (Deering 2007).

[FN265]. Restitution is a remedy that permits a plaintiff to recover funds from a defendant where the plaintiff can demonstrate that the defendant obtained money or property that belonged to the plaintiff. Korea Supply Co. v. Lockheed Martin Corp., 63 P.3d 937, 948 (Cal. 2003).

[FN266]. See Cal. Bus. & Prof. Code § 17206 (Deering 2007).

[FN267]. See Merlo v. Standard Life & Acc. Ins. Co., 130 Cal. Rptr 416 (Cal. Ct. App. 1976).

[FN268]. See Cacique, Inc. v. Robert Reiser & Co., 169 F.3d 619, 624 (9th Cir. 1999) (disallowing use of UCL in trade secrets case to recover royalties); see also Xerox Corp. v. Apple Computer, Inc., 734 F. Supp. 1542, 1550 (N.D. Cal. 1990).

[FN269]. Bank of the West v. Superior Court, 833 P.2d 545 (Cal. 1992).

[FN270]. Cortez v. Purolator Air Filtration Prods. Co., 999 P.2d 706, 709 (2000) (holding that a court may not disgorge all of defendant's profits, but may only order restitution to individuals who have lost money or property as a result of defendant's wrongful conduct).

[FN271]. Korea Supply Co. v. Lockheed Martin Corp., 63 P.3d 937, 937-38 (Cal. 2003). In Korea Supply, the plaintiff, an arm's broker, was hired to promote a bid to the Republic of Korea. The contract was awarded to a competitor, Lockheed Martin. The plaintiff argued that the contract was procured by improper means. The appellate court agreed stating that the profits earned by defendant by improper means could be recovered by plaintiff, where plaintiff would have otherwise obtained these profits.

[FN272]. Cal. Civ. Code § 1747.08(b) (Deering 2007) (“For purposes of this section ‘personal identification information,’ means information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number.”).

[FN273]. Id. § 1747.08(a)(1)-(3).

[FN274]. Id. § 1747.08(c)(1)-(4).

[FN275]. Id. § 1747.08(d).

[FN276]. Id. § 1747.08(d).

[FN277]. Id. § 1747.08(e).

[FN278]. Id.

[FN279]. Id.

[FN280]. Id. § 1747.08(f).

[FN281]. Id.

[FN282]. Id.

[FN283]. Party City Corp. v. Superior Court, 86 Cal. Rptr. 3d 721, 723 (Cal. Ct. App. 2008).

[FN284]. Id. at 737.

[FN285]. Saulic v. Symantec Corp., 8:07-cv-00610-AHS-PLA, 2009 WL 281479, (C.D. Cal. Jan. 5, 2009) (Internet sales not subject to act); Korn v. Polo Ralph Lauren Corp., No. CIV. S-07-02745 FCD JFM. 2008 WL 2225743 (E.D. Cal. May 28, 2008) (returns not subject to act); TJX Cos., Inc. v. Superior Court, 77 Cal. Rptr. 114, 118-120 (Cal. Ct. App. 2008); Absher v. AutoZone, Inc., 78 Cal. Rptr. 3d 817, 821 (Cal. Ct. App.2008); Romeo v. Home Depot U.S.A., Inc., No. 06CV1505 IEG, 2007 WL 3047105 (S.D. Cal. Oct. 16, 2007).

[FN286]. Thyroff v. Nationwide Mut. Ins. Co., 493 F.3d 109 (2d Cir. 2007).

[FN287]. Burgess v. Am. Express Co., No. 07CVS 40, 2007 WL 2568893, at *2 (N.C. May 21, 2007).

[FN288]. In re TJX Cos. Retail Sec. Breach Litig., 527 F. Supp. 2d 209 (D. Mass. 2007), aff'd in part, 2009 WL 806891 (1st Cir. March 30, 2009).

[FN289]. Trikas v. Universal Card Servs. Corp., 351 F. Supp. 2d 37, 37 (E.D.N.Y. 2005).

[FN290]. Id. at 39.

[FN291]. Id. at 45 (“Here too, however, Plaintiff has not presented sufficient evidence of damages to survive summary judgment. Plaintiff testified that he was never turned down for any credit because of the Bank's actions, and that he never even applied for any credit during the time his account remained erroneously open. Plaintiff admits that he has not suffered monetary damages: ‘It's not a value that I suffered monetarily, as you could say it, a dollar value, because this is, like I said, it's emotional, it's stress, it's burden.”’). For a complete discussion of these concepts and privacy litigation, see generally **Serwin**, supra note 14, at 354-407.

[FN292]. Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004).

[FN293]. Id. at 1197.

[FN294]. Id. at 1199.

[FN295]. Id.

[FN296]. Id. at 1120, see also In re Am. Airlines Privacy Litig., 370 F. Supp. 2d 552 (N.D. Tex. 2005).

[FN297]. Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. Oct. 6, 2005).

[FN298]. Id. at *1.

[FN299]. Id. at *1-2.

[FN300]. Id. at *1.

[FN301]. Id. at *1.

[FN302]. Id. at *4.

[FN303]. Id. at *2.

[FN304]. Id. at *4 ("The Court must acknowledge the important distinction between toxic tort and products liability cases, which necessarily and directly involve human health and safety, and credit monitoring cases, which do not.") (citations omitted).

[FN305]. Id. at *7.

[FN306]. Stollenwerk v. Tri-West Health Care Alliance, No. 05-16990, 254 Fed. Appx. 664, 665-68, (9th Cir. 2007).

[FN307]. Id. at 665.

[FN308]. Forbes v. Wells Fargo Bank, N.A., 420 F. Supp.2d 1018, 1020-21 (D. Minn. 2006).

[FN309]. Id. at 1019.

[FN310]. Id. at 1019-20.

[FN311]. Id. at 4; see also Cox v. Chicago Great W. R. Co., 223 N.W. 675, 677 (Minn. 1929).

[FN312]. Key v. DSW, Inc., 454 F. Supp. 2d 684, 688-69, 66 (S.D. Ohio 2006) ("Therefore, because the specific factual allegations of the Amended Complaint do not allege that the Plaintiff has personally experienced any injury other than 'hav[ing] been subjected to a substantial increased risk of identity theft or other related financial crimes,' the Court must accept the specific allegations Plaintiff makes as a true representation of the injury that the Plaintiff has suffered.") (citing Inge v. Rock Fin. Corp., 281 F.3d 613 (6th Cir. 2002)).

[FN313]. Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705, 709-10 (S.D. Ohio, 2007).

[FN314]. Id. at 706.

[FN315]. Id. at 707.

[FN316]. Id. at 709.

[FN317]. Id. at 712-13.

[FN318]. See Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 7-8 (D.D.C. 2007) (dismissing claim for future identity theft arising from the theft of a laptop computer).

[FN319]. Schroeder v. Capitol Indem. Corp., 2006 WL 2009053 (E.D. Wis. 2006) (granting summary judgment, in part, and dismissing portion of claim under FCRA because plaintiff failed to evidence of actual injury).

[FN320]. Id. at *5 (citing Murray v. GMAC Mortg. Corp., 434 F.3d 948, 952-53 (7th Cir. 2006)).

[FN321]. In re Am. Airlines, Inc. Privacy Litig., 370 F. Supp. 2d 552, 567 (N.D. Tex. 2005); In re JetBlue Airways Corp. Privacy Litigat., 379 F. Supp. 2d 299, 326-27 (E.D.N.Y. 2005) (holding loss of privacy is not a recoverable damage under a breach of contract theory).

[FN322]. Lujan v. Nat'l Wildlife Fed'n, 504 U.S. 555, 560-61 (1992).

[FN323]. See id. at 561.

[FN324]. See id. at 560; Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 94 (1998); Gerlinger v. Amazon.com, 526 F.3d 1253, 1255 (9th Cir. 2008); Ford v. NYLCare Health Plans of Gulf Coast, Inc., 301 F.3d 329, 332 (5th Cir. 2002) (“Lanham Act prudential standing cannot be addressed so long as Article III standing remains in doubt because constitutional standing is a threshold issue that we should address before examining the issues of prudential standing”) (citing Joint Stock Society v. UDV N. Am., Inc., 266 F.3d 164, 175 (3d Cir. 2001)).

[FN325]. See Steel Co., 523 U.S. at 94 (quoting S. Fire Proof Hotel Co. v. Jones 177 U.S. 449, 453 (1900)).

[FN326]. Bell v. Acxiom, 2006 WL 2850042 at *1 (E.D. Ark. 2006).

[FN327]. Id. at *2 (stating that even if plaintiff had shown that she received junk mail, it is unlikely whether this would have been sufficient showing of injury). In this case, Plaintiff alleged that she suffered an increased risk of both receiving unsolicited mailing advertisements and of identity theft. In response, Defendant argues that both Plaintiff's alleged injuries are speculative--Plaintiff has not plead that she has received a single marketing mailer or had her identity stolen. Moreover, several courts have held that the receipt of unsolicited and unwanted mail does not constitute actual harm. Additionally, while there have been several lawsuits alleging an increased risk of identity theft, no court has considered the risk itself to be damage. Only where the plaintiff has actually suffered identity theft has the court found that there were damages. Furthermore, Plaintiff does not know whether her name and information were contained within the databases stolen by Levine. More than three years after the theft, Plaintiff has not alleged that she has suffered anything greater than an increased risk of identity theft. Because Plaintiff has not alleged that she has suffered any concrete damages, she does not have standing under the case or controversy requirement.

See also, Walters v. DHL Exp., 2006 WL 1314132 *1,*5 (C.D. Ill. 2006) (dismissing case based upon damage claim for increased risk of identity theft); Smith v. Chase Manhattan Bank, USA, 741 N.Y.S.2d 100 (N.Y. App. Div. 2002) (receipt of unsolicited advertisements did not constitute actual harm); Shibley v. Time, Inc.,

341 N.E.2d 337, 339-40 (Ohio Ct. App. 1975) (the "right of privacy does not extend to the mailbox"); c.f. Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003) (damages existed when private investigator sold information to an individual who was stalking a person that he ultimately killed because the court concluded that the private investigator, in these circumstances, had a duty not to subject a third party to an increased risk of criminal misconduct).

[FN328]. Levine v. DSW, Inc., Court of Common Pleas, State of Ohio, County of Cuyhoga, Civil Case No. 586371 (2008).

[FN329]. Biddle v. Warren Gen. Hosp., 75 N.E.2d 518, 523-24 (Ohio 1999).

[FN330]. State ex rel. Office of Montgomery County Pub. Defender v. Siroki, 842 N.E.2d 508, 511-12 (Ohio 2006); Beacon Journal Publ'g Co. v. City of Akron, 640 N.E.2d 164, 169 (Ohio 1994).

[FN331]. Pichler v. UNITE, 542 F.3d 380, 383 (3d Cir. 2008).

[FN332]. Id. at 384.

[FN333]. Id.

[FN334]. Holding that in order to meet the standing requirement the plaintiff must show three things. "First, the plaintiff must have suffered an injury in fact-an invasion of a legally protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of-the injury has to be fairly traceable to the challenged action of the defendant, and not the result of some third party not before the court. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." Id. at 390-91 (citing Lujan v. Nat'l Wildlife Fed'n, 504 U.S. 555, 560-61 (1992) (quotation marks, footnote, and citations omitted)).

[FN335]. Id. at 391-392.

[FN336]. See, e.g., Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).

[FN337]. Id. at 634.

[FN338]. Id. at 636-40.

[FN339]. See, e.g., Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273 (S.D.N.Y. 2008)

[FN340]. Id. at 280.

[FN341]. Ruiz v. Gap, Inc., 2009 WL 941162 (N.D. Cal. 2009).

[FN342]. Id. at *1.

[FN343]. Id. at *4.

[FN344]. See Lujan v. Nat'l Wildlife Fed'n, 504 U.S. 555, 561 (1992).

[FN345]. 47 U.S.C. § 230 (2006).

[FN346]. H.R. Rep. No.104-458 at 188-189 (1996), reprinted in 1996 U.S.C.C.A.N 10.

[FN347]. Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1164-65 n.15 (9th Cir. 2008) ("The dissent stresses the importance of the Internet to modern life and commerce, Dissent at 1176, and we, of course, agree: The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant-perhaps the preeminent-means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.").

[FN348]. Id. at 1163.

[FN349]. Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. App. Div. 1995).

[FN350]. Fair Housing Council, 521 F.3d at 1157 (quoting H.R. Rep. No. 104-458 (1996)).

[FN351]. Associated Bank-Corp. v. Earthlink, Inc., 2005 WL 2240952, at *3 (W.D. Wis. 2005).

[FN352]. Id.

[FN353]. "Interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions. 47 U.S.C. §230(f)(2) (2006).

[FN354]. Id. § 230(c)(1). "Information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service. Id. § 230(f)(3).

[FN355]. Id. § 230(c)(2).

[FN356]. Carafano v. Metrosplash.com Inc., 207 F. Supp. 2d 1055, 1064 (C.D. Cal. 2002), aff'd on other grounds, 339 F.3d 1119 (9th Cir. 2003); see also Blumenthal v. Drudge, 992 F. Supp. 44, 51-52 (D.D.C. 1998) (service provider's retention of editorial right, even if not exercised, did not preclude CDA immunity); Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003).

[FN357]. Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007).

[FN358]. Carafano, 207 F. Supp. 2d at 1066.

[FN359]. These included: breach of contract; fraud; negligent infliction of emotional distress; negligent misrepresentation; breach of warranty; violation of the Ohio Consumer Sales Practices Act; and failure to warn. Doe v. SexSearch.com, 502 F. Supp. 2d 719, 724, 728 (N.D. Ohio 2007).

[FN360]. FTC v. Accusearch, Inc., 2007 WL 4356786 at *5 (D. Wyo. 2007).

[FN361]. Anthony v. Yahoo!, 421 F. Supp. 2d 1257, 1263 (N.D. Cal. 2006).

[FN362]. Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 536 (D. Md. 2006).

[FN363]. Id. at 528.

[FN364]. Id. at 529.

[FN365]. Id. at 537.

[FN366]. Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1161 (9th Cir. 2008).

[FN367]. Id. at 1162.

[FN368]. Id. at 1166.

[FN369]. Id. at 1161.

[FN370]. Id. at 1167.

[FN371]. Id. at 1167.

[FN372]. Id. at 1165.

[FN373]. Id. (“The salient fact in Carafano was that the website's classifications of user characteristics did absolutely nothing to enhance the defamatory sting of the message, to encourage defamation or to make defamation easier: The site provided neutral tools specifically designed to match romantic partners depending on their voluntary inputs. By sharp contrast, Roommate's website is designed to force subscribers to divulge protected characteristics and discriminatory preferences, and to match those who have rooms with those who are looking for rooms based on criteria that appear to be prohibited by the FHA.”) Id. at 1172.

[FN374]. Id. at 1165 (noting that this portion of its holding was consistent with its prior holding in Batzel v. Smith, 333 F.3d 1018, 1033 (9th Cir. 2003)); see also Anthony v. Yahoo Inc., 421 F. Supp. 2d 1257, 1263-64 (N.D. Cal. 2006).

[FN375]. Roommates.com, 521 F.3d at 1173-74 (“Roommate publishes these comments as written. It does not provide any specific guidance as to what the essay should contain, nor does it urge subscribers to input discriminatory preferences. Roommate is not responsible, in whole or in part, for the development of this content, which comes entirely from subscribers and is passively displayed by Roommate. Without reviewing every essay, Roommate would have no way to distinguish unlawful discriminatory preferences from perfectly legitimate statements. Nor can there be any doubt that this information was tendered to Roommate for publication online. This is precisely the kind of situation for which section 230 was designed to provide immunity.”) (internal citations omitted).

[FN376]. Id. at 1167.

[FN377]. Id.

[FN378]. Id.

[FN379]. Id. at 1170.

[FN380]. Id. at 1170 (“Our opinion is entirely consistent with that part of Batzel which holds that an editor's minor changes to the spelling, grammar and length of third-party content do not strip him of section 230 immunity. None of those changes contributed to the libelousness of the message, so they do not add up to ‘development’ as we interpret the term.”).

[FN381]. Id. at 1170-71 (“The distinction drawn by Batzel anticipated the approach we take today. As Batzel explained, if the tipster tendered the material for posting online, then the editor's job was, essentially, to determine whether or not to prevent its posting-precisely the kind of activity for which section 230 was meant to provide immunity. And any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230. But if the editor publishes material that he does not believe was tendered to him for posting online, then he is the one making the affirmative decision to publish, and so he contributes materially to its allegedly unlawful dissemination. He is thus properly deemed a developer and not entitled to CDA immunity.”) (internal citations and footnotes omitted).

[FN382]. Id. at 1171 (quoting Carafano v. Metrosplash.com. Inc., 339 F.3d 1119, 1124 (9th Cir. 2003)).

[FN383]. Id. at 1171 n.31.

[FN384]. Id. at 1171.

[FN385]. Doe v. MySpace, Inc., 528 F.3d 413, 418 (5th Cir. 2008).

[FN386]. Id. at 422.

[FN387]. Roommates.com, 521 F.3d at 1164.

[FN388]. Energy Automation Sys. v. Xcentric Ventures, LLC, 2007 WL 1557202 at * 11 (M.D. Tenn. 2007).

[FN389]. 47 U.S.C. §230(d) (2000).

[FN390]. Id.

[FN391]. FED. R. CIV. P. 23(a).

[FN392]. FED. R. CIV. P. 23(b).

[FN393]. Hannon v. Data Prods. Corp., 976 F.2d 497, 508 (9th Cir. 1992) (citing Weinberger v. Thornton, 114 F.R.D. 599, 603 (S.D. Cal. 1986)).

[FN394]. Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 625 (1997); Lerwill v. Inflight Motion Pictures, Inc., 582 F.2d 507, 512 (9th Cir. 1978).

[FN395]. Fed. R. Civ. P. 23(a).

[FN396]. “Impracticable does not mean impossible,” however, and “the numerosity requirement is satisfied when joinder of all putative class members would needlessly complicate and hinder efficient resolution of the litigation.” Karvaly v. eBay, Inc., 245 F.R.D. 71, 80 (E.D.N.Y. 2007) (quoting Trief v. Dun & Bradstreet Corp.,

144 F.R.D. 193, 198 (S.D.N.Y. 1992)); Robidoux v. Celani, 987 F.2d 931, 935 (2d Cir. 1993); Parker v. Time Warner Entm't Co., L.P., 239 F.R.D. 318, 329 (E.D.N.Y. 2007); In re Initial Public Offering Sec. Litig., 227 F.R.D. 65, 86 (S.D.N.Y. 2004); Consolidated Rail Corp. v. Town of Hyde Park, 47 F.3d 473, 482-83 (2d Cir. 1995).

[FN397]. See, e.g., In re Medical X-Ray Firm Antitrust Litig., 1997 WL 33320580, at *3 (E.D.N.Y. Dec. 16, 1997) (finding numerosity prong satisfied where "the total class size would amount to about 2000 dealers, hospitals, and other direct purchasers that are geographically dispersed across the country"); In re Indep. Energy Holdings PLC Sec. Litig., 210 F.R.D. 476, 479 (S.D.N.Y. 2002) (finding numerosity prong satisfied where "thousands of investors engaged in transactions during the Class Period involving the securities that are the subject of this litigation"). Moreover, the Second Circuit has recognized that "numerosity is presumed at a level of 40 members," Consolidated Rail Corp, 47 F.3d at 483; Robidoux, 987 F.2d at 936; Indep. Energy, 210 F.R.D. at 479 ("While precise calculation of the number of class members is not required, numbers in excess of forty generally satisfy the requirement.") (citations omitted).

[FN398]. Karvaly, 245 F.R.D. at 81 (quoting Marisol A. v. Giuliani, 126 F.3d 372, 376 (2d Cir. 1997)).

[FN399]. Lewis Tree Serv., Inc. v. Lucent Techs. Inc., 211 F.R.D. 228, 231 (S.D.N.Y. 2002).

[FN400]. Kamean v. Local 363, Int'l Bhd. of Teamsters, 109 F.R.D. 391, 394 (S.D.N.Y. 1986).

[FN401]. Lewis Tree, 211 F.R.D. at 232 (finding commonality not present where the party "has merely construed the factual basis of each class member's claim in the most general fashion ... [and] has not alleged that [the] products [at issue], and their multiple versions, were similar in any respect, beyond the fact that they all purportedly contained Y2K defects and were telecommunications products") (quoting Sprague v. Gen. Motors Corp., 133 F.3d 388, 397 (6th Cir. 1998)).

[FN402]. Parker v. Time Warner Entm't Co., 239 F.R.D. 318, 329 (E.D.N.Y 2007) ("[T]he commonality and typicality requirements 'tend to merge, because [b]oth serve as guideposts for determining whether ... the named plaintiff's claim and the class claims are so inter-related that the interests of the class members will be fairly and adequately protected in their absence."') (quoting Caridad v. Metro-North Commuter R.R., 191 F.3d 283, 291 (2d Cir. 1999)).

[FN403]. Parker, 239 F.R.D. at 329.

[FN404]. Caridad, 191 F.3d at 293 (quoting Krueger v. N.Y. Tel. Co., 163 F.R.D. 433, 442 (S.D.N.Y. 1995)).

[FN405]. Kamean, 109 F.R.D. at 394; see also In re Medical X-Ray Film Antitrust Litig., 1997 WL 33320580, at *4 (E.D.N.Y. Dec. 16, 1997); In re Prudential Sec. Inc. Ltd. P'ships Litig., 163 F.R.D. 200, 208 (S.D.N.Y. 1995).

[FN406]. Cooper v. S. Co., 390 F.3d 695, 714 (11th Cir. 2004) (quoting Appleyard v. Wallace, 754 F.2d 955, 958 (11th Cir. 1985)); see also Hanlon v. Chrysler Corp., 150 F.3d 1011, 1020 (9th Cir. 1998) ("Under [Rule 23(a)(3)'s] permissive standards, representative claims are 'typical' if they are reasonably co-extensive with those of absent class members; they need not be substantially identical.").

[FN407]. Karvaly v. eBay, Inc., 245 F.R.D. 71 (E.D.N.Y. 2007) (quoting In re W. Union Money Transfer Litig., 2004 WL 3709932, at *15 (E.D.N.Y. 2004)).

[FN408]. Parker, 239 F.R.D. at 330 (quoting In re LILCO Secs. Litig., 111 F.R.D. 663, 672 (E.D.N.Y. 1986)).

[FN409]. Id. (quoting LILCO Secs. Litig., 111 F.R.D. at 672).

[FN410]. Unger v. Amedisys, Inc., 401 F.3d 316, 320 (5th Cir. 2005) (citing Berger v. Compaq Computer Corp., 257 F.3d 475, 479 (5th Cir. 2001)); In re Medical X-Ray Film Antitrust Litig., 1997 WL 33320580, at *3 (E.D.N.Y. 1997).

[FN411]. Gen. Tel. Co. v. Falcon, 457 U.S. 147, 157 n.13 (1982); Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 626 n.20 (1997); Armstrong v. Davis, 275 F.3d 849, 868 (9th Cir. 2001) (quoting Marisol v. Giuliani, 126 F.3d 372, 376 (2d Cir. 1997) ("The crux of [commonality and typicality] requirements is to ensure that 'maintenance of a class action is economical and [that] the named plaintiff's claim and the class claims are so interrelated that the interests of the class members will be fairly and adequately protected in their absence."')).

[FN412]. Eisen v. Carlisle & Jacquelin, 417 U.S. 156, 177 (1974); Miller v. Mackey Int'l, Inc. 452 F.2d 424, 427 (5th Cir. 1971); See Valentino v. Carter-Wallace, Inc., 97 F.3d 1227, 1232 (9th Cir. 1996); Hudson v. Delta Air Lines, Inc., 90 F.3d 451, 457 (11th Cir. 1996); Adamson v. Bowen, 855 F.2d 668, 676 (10th Cir. 1988); McCarthy v. Kleindienst, 741 F.2d 1406, 1414 n.8 (D.C. Cir. 1984); Redditt v. Miss. Extended Care Ctr, Inc., 718 F.2d 1381, 1388 (5th Cir. 1983); Sirota v. Solitron Devices, Inc., 673 F.2d 566, 570 (2d Cir. 1982); Eggleston v. Chi. Journeymen Plumbers, etc., 657 F.2d 890, 895 (7th Cir. 1981); Finberg v. Sullivan, 634 F.2d 50, 64 (3d Cir. 1980); Doctor v. Seaboard Coast Line R.R., 540 F.2d 699, 707 (4th Cir. 1976); Weathers v. Peters Realty Corp., 499 F.2d 1197, 1201 (6th Cir. 1974); see Lamphere v. Brown Univ., 553 F.2d 714, 718 n.11 (1st Cir. 1977).

[FN413]. Teamsters Local 445 Freight Div. Pension Fund v. Bombardier, Inc., 2006 WL 2161887, at *4 (S.D.N.Y. 2006), aff'd, 546 F.3d 196 (2d Cir. 2008).

[FN414]. Harris v. Palm Springs Alpine Estates, Inc., 329 F.2d 909 (9th Cir. 1964).

[FN415]. Cole v. GM Corp., 484 F.3d 717, 723 (5th Cir. 2007); Karvaly v. eBay, Inc., 245 F.R.D. 71 (E.D.N.Y. 2007).

[FN416]. Klender v. United States, 218 F.R.D. 161, 166-67 (E.D. Mich. 2003) (citing Coleman v. Gen. Motors Acceptance Corp., 296 F.3d 443, 447 (6th Cir. 2002)).

[FN417]. Id. at 168 (citing Coleman, 296 F.3d at 448).

[FN418]. FED. R. CIV. P. 23(b)(1).

[FN419]. FED. R. CIV. P. 23(b)(2).

[FN420]. Molski v. Gleich, 318 F.3d 937, 947 (9th Cir. 2003).

[FN421]. Dukes v. Wal-Mart, Inc., 509 F.3d 1168, 1186 (9th Cir. 2007).

[FN422]. FED. R. CIV. P. 23(b)(3).

[FN423]. Amchem Prods. Inc. v. Windsor, 521 U.S. 591, 594 (1997).

[FN424]. FED. R. CIV. P. 23(b)(3).

[FN425]. Id.

[FN426]. Amchem, 521 U.S. at 614.

[FN427]. Klender v. United States, 218 F.R.D. 161, 167 (E.D. Mich. 2003) (citing In re Dennis Greenman Secs. Litig., 829 F.2d 1539, 1545 (11th Cir. 1987)); Bacon v. Honda of Am. Mfg., Inc., 205 F.R.D. 466, 483 (S.D.Ohio 2001).

[FN428]. Amchem, 521 U.S. at 614.

[FN429]. Id. (citing Fed. R. Civ. P. 23 advisory committee's note to 1996 amendment).

[FN430]. Parker v. Time Warner Entm't Co., L.P., 239 F.R.D. 318, 331 (E.D.N.Y. 2007) (quoting Fed. R. Civ. P. 23 advisory committee's note to 1996 amendment).

[FN431]. Robinson v. Metro-North Commuter R.R., 267 F.3d 147, 164 (2d Cir. 2001).

[FN432]. Id.

[FN433]. Parker v. Time Warner Entm't Co., L.P., 331 F.3d 13, 20 (2d Cir. 2003) (citing Robinson, 267 F.3d at 164).

[FN434]. Id.

[FN435]. In re Nassau County Strip Search Cases, 461 F.3d 219, 225 (2d Cir. 2006) (quoting In re Visa Check/ MasterMoney Antitrust Litig., 280 F.3d 124, 136 (2d Cir. 2001)); see also Amchem Prods. Inc. v. Windsor, 521 U.S. 591, 623 (1997).

[FN436]. Moore v. Painewebber, Inc., 306 F.3d 1247, 1252 (2d Cir. 2002).

[FN437]. See id.; Karvaly v. eBay, Inc., 245 F.R.D. 71, 84 (E.D.N.Y. 2007).

[FN438]. Amchem, 521 U.S. at 624-25 (quoting Georgine v. Amchem Prods., Inc., 83 F.3d 610, 626 (3d Cir. 1996) aff'd 521. U.S. 591 (1997)).

[FN439]. Karvaly, 245 F.R.D. at 84.

[FN440]. Parker v. Time Warner Entm't Co., L.P., 239 F.R.D. 318, 334 (E.D.N.Y. 2007); see also In re Nissan Motor Corp. Antitrust Litig., 552 F.2d 1088 (5th Cir. 1977); Abrams v. Interco Inc., 719 F.2d 23, 30 (2d Cir. 1983); Besinga v. United States, 923 F.2d 133 (9th Cir. 1991).

[FN441]. Parker, 239 F.R.D. at 334.

[FN442]. Castano v. Am. Tobacco Co., 84 F.3d 734, 745 (5th Cir. 1996); Simon v. Merrill Lynch., 482 F.2d 880, 882 (5th Cir. 1973).

[FN443]. Parker, 239 F.R.D. at 320.

[FN444]. Id.

[FN445]. Id. at 321.

[FN446]. Id.

[FN447]. Id. at 342.

[FN448]. See, e.g., Cal. Civ. P. Code § 382 (Deering 2008).

[FN449]. Wash. Mut. Bank, v. Superior Court, 15 P.3d 1071, 1076 (Cal. 2001) (citing San Jose v. Superior Court, 525 P.2d 701, 710 (Cal. 1974)); Linder v. Thrifty Oil, 2 P.3d 27, 31 (Cal. 2000) ("By establishing a technique whereby the claims of many individuals can be resolved at the same time, the class suit both eliminates the possibility of repetitious litigation and provides small claimants with a method of obtaining redress .... Generally, a class suit is appropriate when numerous parties suffer injury of insufficient size to warrant individual action and when denial of class relief would result in unjust advantage to the wrongdoer. But because group action also has the potential to create injustice, trial courts are required to carefully weigh respective benefits and burdens and to allow maintenance of the class action only where substantial benefits accrue both to litigants and the courts.") (internal quotations and citations omitted).

[FN450]. San Jose, 525 P.2d at 709; see also Kennedy v. Baxter Heathcare Corp., 43 Cal. App. 4th 799, 810 (Cal. Ct. App. 1996).

[FN451]. These elements are at times framed in different ways, all courts require the same elements, though some are framed as sub-elements. "Section 382 of the Code of Civil Procedure authorizes class suits in California when the question is one of a common or general interest, of many persons, or when the parties are numerous, and it is impracticable to bring them all before the court. To obtain certification, a party must establish the existence of both an ascertainable class and a well-defined community of interest among the class members. The community of interest requirement involves three factors: (1) predominant common questions of law or fact; (2) class representatives with claims or defenses typical of the class; and (3) class representatives who can adequately represent the class. Other relevant considerations include the probability that each class member will come forward ultimately to prove his or her separate claim to a portion of the total recovery and whether the class approach would actually serve to deter and redress alleged wrongdoing." Linder, 2 P.3d at 31 (internal quotations and citations omitted). In reality, California Courts borrow from the Federal Rules regarding the elements necessary to satisfy a class action.

[FN452]. See Richmond v. Dart Indus., Inc., 629 P.2d 23, 27-28 (Cal. 1981); Vasquez v. Superior Court, 484 P.2d 964, 969 (Cal. 1971).

[FN453]. Reyes v. Board of Supervisors, 196 Cal. App. 3d 1263, 1270-71 (Cal. Ct. App. 1987).

[FN454]. Id. at 1274.

[FN455]. See Hypolite v. Carelson, 52 Cal. App. 3d 566, 578 (Cal. Ct. App. 1975).

[FN456]. See Daar v. Yellow Cab. Co., 433 P.2d 732, 740 (Cal. 1967).

[FN457]. Weaver v. Pasadena Tournament of Roses Asso., 198 P.2d 514, 517, 519 (Cal. 1948).

[FN458]. Richmond v. Dart Indus. Inc., 629 P.2d 23, 28 (Cal. 1981); see also Reese v. Wal-Mart Stores, Inc., 73

Cal. App. 4th 1225, 1234 (Cal. Ct. App. 1999).

[FN459]. Caro v. Proctor & Gamble, 18 Cal. App. 4th 644, 667-68 (Cal. Ct. App. 1993) (quoting Vasquez v. Superior Court, 484 P.2d 964, 970 (Cal. 1971)).

[FN460]. See San Jose v. Superior Court, 525 P.2d 701, 709 (Cal. 1974).

[FN461]. McGhee v. Bank of Am., 60 Cal. App. 3d 442, 449 (Cal. Ct. App. 1976).

[FN462]. See Wilens v. TD Waterhouse Group, Inc., 120 Cal. App. 4th 746, 756 (Cal. Ct. App. 2003).

[FN463]. Id.

[FN464]. Id.

[FN465]. B.W.I. Custom Kitchen v. Owens-Illinois, Inc., 191 Cal.App.3d 1341, 1347 (Cal. Ct. App. 1987).

[FN466]. See Classen v. Weller, 145 Cal. App. 3d 27, 46 (Cal. Ct. App. 1983); Global Minerals & Metals Corp. v. Superior Court, 113 Cal. App. 4th 836, 851 (Cal. Ct. App. 2004) (citing Lockheed Martin Corp. v. Superior Court, 63 P.3d 913, 918 (Cal. 2003)).

[FN467]. Caro v. Proctor & Gamble Co., 18 Cal. App. 4th 644, 663 (Cal. Ct. App. 1993) (“[t]he cases uniformly hold that a plaintiff seeking to maintain a class action must be a member of the class he claims to represent”) (citing Chern v. Bank of Am., 544 P.2d 1310, 1315 (Cal. 1976)); see Caro, 18 Cal. App. 4th at 662 (The determination that a representative plaintiff's claims are atypical of the class, on its own, is “sufficient to defeat class certification” under Code of Civil Procedure §382 and the CLRA.).

[FN468]. Caro, 18 Cal. App. 4th at 666.

[FN469]. Caro, 18 Cal. App. 4th at 664.

[FN470]. Caro, 18 Cal. App. 4th at 664-65; Chern, 544 P.2d at 1315 (if the plaintiff was not misled, she cannot represent those who were); see also Starbucks v. Superior Court, 168 Cal. App. 4th 1436, 1447-48 (Cal. Ct. App. 2008) (holding dismissal was proper because the named plaintiffs had not been convicted of the relevant marijuana offenses and had also read and understood the disclaimer, and therefore did not represent the proposed class).

[FN471]. Global Minerals, 113 Cal. App. 4th at 854 (citing Lockheed Martin, 63 P.3d at 918).

[FN472]. La Sala v. Am. Sav. & Loan Assn., 480 P.2d 1113, 1117 (Cal. 1971).

[FN473]. See Cal Pak Delivery, Inc. v. UPS, Inc., 52 Cal. App. 4th 1, 12 (Cal. Ct. App. 1997).

[FN474]. See id.

[FN475]. Blue Chip Stamps v. Superior Court, 556 P.2d 755, 385 (Cal. 1976) (citing San Jose v. Superior Court, 525 P.2d 701, 709 (Cal. 1974)).

[FN476]. Green v. Obledo, 624 P.2d 256, 268 (Cal. 1981).

[FN477]. Quacchia v. DaimlerChrysler Corp., 122 Cal. App. 4th 1442, 1454 (Cal. Ct. App. 2004).

[FN478]. This statute was previously numbered as § 1748.8.

[FN479]. Linder v. Thrifty Oil, 2 P.3d 27 (Cal. 2000).

[FN480]. Id. at 30.

[FN481]. Id.

[FN482]. Id.

[FN483]. Id. at 37 ("The trial court denied class certification for the additional reason that class members would not receive any substantial benefit. While the court did not address potential recoveries of penalty class members, it did conclude that the individual damages of surcharge class members, if any, 'would be small, perhaps not enough to support the required mailings to and from the class.' The Court of Appeal agreed, finding that the surcharge claim, even if legally correct, would not confer substantial benefits because the burden of identifying class members and providing notice would be too high in relation to the small amount of the potential recovery.").

[FN484]. Id. at 38 (citing Vasquez v. Superior Court, 484 P.2d 964, 968-69 (Cal. 1971)).

[FN485]. Id. at 39 ("While the potential amount of each individual recovery is a significant factor in weighing the benefits of a class action, it is not the only factor requiring consideration. By incorrectly limiting the scope of the relevant inquiry, the lower courts here did not evaluate whether the proposed class suit is the only effective way to halt and redress the alleged wrongdoing, or to prevent unjust advantage to Thrifty. Moreover, the Court of Appeal assumed that substantial time and expense would be required to provide legally adequate notice to class members, even though the trial court had yet to take evidence and rule on the matter. Accordingly, without intimating any view on the matter, we find it appropriate to leave this issue to the trial court for reexamination.").

[FN486]. Holster v. Gatco, Inc., 485 F. Supp. 2d 179, 185 (E.D.N.Y. 2007) (finding New York law did not permit class actions under the TCPA).

[FN487]. Kaufman v. ACS Sys., Inc., 110 Cal. App. 4th 886, 925 (Cal. Ct. App. 2003) (finding that class actions under the TCPA could be permissibly brought if California's class action requirements were met).

[FN488]. See McGaughey v. Treistman, 2007 WL 24935 at *3 (S.D.N.Y. Jan. 4, 2008).

[FN489]. Forman v. Data Transfer, Inc., 164 F.R.D. 400, 403 (E.D. Penn. 1995) (denying class certification and stating that "courts have been unwilling to find commonality where the resolution of 'common issues' depends on factual determinations that will be different for each class plaintiff").

[FN490]. Id. at 404 ("Although plaintiff relies on the same legal theory as the purported class, namely 47 U.S.C. § 227, as discussed with regard to the commonality question, his claims do not arise from the same event or course of conduct that gives rise to the claims of the class members.")

[FN491]. See id.

[FN492]. Hinman v. M & M Rental Ctr., Inc., 545 F. Supp. 2d 802, 804 (N.D. Ill. 2008).

[FN493]. Melancon v. La. Office of Student Fin. Assistance, 567 F. Supp. 2d 873, 877 (E.D. La. 2008) (rejecting class action arising from alleged loss of data because damages were speculative).

[FN494]. See Pioneer Elecs. (USA), Inc., v. Superior Court, 150 P.3d 198, 199 (Cal. 2007).

[FN495]. Id. at 201.

[FN496]. Id. at 204 (citing Hills v. Nat'l Collegiate Athletic Ass'n, 856 P.2d 633, 654-55 (Cal. 1994)).

[FN497]. Id. at 201 (Colonial Life letters refer to the process identified in the insurance arena for disclosure of other insureds pursuant to the California Supreme Court's holding in Colonial Life & Accident Ins. Co. v. Superior Court, 647 P.2d 86 (1982)).

[FN498]. See id. at 205-06.

[FN499]. Id. at 205, 207.

[FN500]. Crab Addison v. Superior Court, 169 Cal. App. 4th 958, 967 (Cal. Ct. App. 2008).

[FN501]. Id. at 961.

[FN502]. Id. at 962-63.

[FN503]. Id. at 963.

[FN504]. Puerto v. Superior Court, 158 Cal. App. 4th 1242 (Cal. Ct. App. 2008).

[FN505]. Crab Addison, 169 Cal. App. 4th at 966 (citing Puerto, 158 Cal. App. 4th at 1250-51).

[FN506]. Puerto, 158 Cal. App. 4th at 1253-54 (quoting Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 655 (Cal. 1994)).

[FN507]. Crab Addison, 169 Cal. App. 4th at 970.

[FN508]. Alch v. Superior Court, 165 Cal. App. 4th 1412 (Cal. Ct. App. 2008).

[FN509]. Id. at 1416.

[FN510]. Id.

[FN511]. Id.

[FN512]. See id. at 1418.

[FN513]. See id. at 1436.

[FN514]. Id. at 1423.

[FN515]. Id. (quoting Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 654 (Cal. 1994)).

[FN516]. Id. (quoting Hill, 865 P.2d at 655).

[FN517]. Id. (quoting Hill, 865 P.2d at 655).

[FN518]. Id. at 1423-24 (quoting Pioneer Elecs. (USA), Inc. v. Superior Court, 150 P.3d 198, 204 (Cal. 2007)).

[FN519]. Id. at 1425 (quoting Britt v. Superior Court, 574 P.2d 766, 775(Cal. 1978)).

[FN520]. Compare Alch, 165 Cal. App. 4th at 1433, with Harding Lawson Assocs. v. Superior Court, 10 Cal. App. 4th 7, 10 (Cal. Ct. App. 1992) (holding that the trial court's discovery order was overbroad and unjustified because it required the production of confidential information contained in personnel files of employees other than the plaintiff and that the plaintiff had not shown a compelling need for the particular confidential documents in the third-party personnel files), and Bd. of Trustees. v. Superior Court, 119 Cal. App. 3d 516, 526 (Cal. Ct. App. 1981).

[FN521]. Alch, 165 Cal. App. 4th at 1435; see Pureto v. Superior Court, 158 Cal. App. 4th 1242, 1253 (Cal. Ct. App. 2008).

[FN522]. CashCall v. Superior Court, 159 Cal. App. 4th 273, 278, 280 (Cal. Ct. App. 2008).

[FN523]. Id. at 280.

[FN524]. Id. at 281.

[FN525]. “We conclude the trial court did not abuse its discretion in applying the Parris balancing test and concluding the rights and interests of the class members outweighed the potential for abuse of the classaction procedure in the circumstances of this case. In deciding whether to grant or deny a motion for precertification discovery of the identities of class members, a trial court, in applying the Parris balancing test, “must ... expressly identify any potential abuses of the classaction procedure that may be created if the discovery is permitted, and weigh the danger of such abuses against the rights of the parties under the circumstances.” Id. at 292 (citing Parris v. Superior Court, 109 Cal. App. 4th 285, 301 (Cal. Ct. App. 2003).
25 Santa Clara Computer & High Tech. L.J. 883

END OF DOCUMENT