ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

A Crash-Course in Data-Security Regulation and Litigation

Litigation and Dispute Resolution

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***A federal void.*** Despite the exponential growth of cyber-attacks, the United States still does not have a unified set of federal data security regulations.
- ***A plethora of state regulations.*** Without any overarching federal regime, state laws are currently the primary source of cybersecurity regulation. California offers a common template for other states' laws.
- ***A diverse set of threats.*** The government is not the only threat in the aftermath of a data breach. Arbitration clauses and challenging a lawsuit based on a lack of standing are two common defenses to consumer class action litigation.
- ***Our suggestions.*** Nimbly navigate the post-data breach legal landscape with these 10 tips to reduce risk.

It happened. An employee left a laptop with sensitive customer information in a local coffee shop, where it was stolen. Or perhaps a hacker broke into your company's secured server and extracted confidential customer information. Either way, your data security is compromised, you have a public relations disaster on your hands, and you are struggling to figure out how far the damage extends. While this article focuses on failing to protect customer information, the risk is even larger when you consider confidential employee information or other private internal data.

And make no mistake about it — it can happen to you. No business is too big or too small to escape data security issues. According to one report, in the first three months of 2013 alone, there were over one billion Internet-based cyber-attacks. Forty percent were against small businesses. That translates into more than 51 cyberattacks on small businesses every second. On the flip side, major retailers like Target and Barnes & Noble have also been high-profile victims of data security hacks. The government is also not immune: the Office of Personnel Management ("OPM") announced this year that it was the victim of two critical cyberattacks: one potentially compromising the information of over 4 million people, and the other involving high-level security information of key government workers. And these are just the reported attacks. When one considers unreported and undiscovered breaches, the true number of cyber-attacks is likely exponentially larger.

Being the target of a cyber-attack is something no company or organization ever wants to experience. The only thing that's worse? Being sued for being the target of a cyber-attack.

Unfortunately, that is a very real risk in the rapidly expanding world of data-security litigation. As the number of data breaches has grown, so has the number of cases brought by both regulatory agencies and plaintiff's lawyers. Whether or not your company is actually sued — and how much you end up paying in any settlement negotiations — depends in part on how well you know the legal terrain. This article offers in-house counsel a crash-course in data-security regulation and litigation, focusing on the liabilities stemming from the disclosure of customers' personally identifying information (PII). We will conclude by examining some key takeaways to help your company minimize its data-security litigation risk.

Overview of data privacy regulations

Federal regulations

Despite the exponential growth of cyber-attacks, the United States still does not have a unified set of federal data security regulations. While there are a few bills pending, such as the Data Security and Breach Notification Act of 2015 (S.177), they face party division. Democrats fear a weak federal data security standard replacing strong state laws, while Republicans fear intrusive federal regulations. Hopefully, the recent OPM breach will spur cross-party coordination on this important issue.

In the meantime, current federal law only protects specific kinds of information in specific industries. For example, The Children's Online Privacy Protection Act of 1998 (COPPA) imposes certain requirements on online operators handling the PII of children under 13 years old. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates personal health information, while the Fair and Accurate Credit Transactions Act of 2003 (FACTA) regulates consumer account information.

Because there are no specific federal regulations governing cybersecurity, Section 5 of the FTC Act has emerged as the principle federal statue in this arena. The FTC prosecutes cybersecurity breaches under Section 5 by alleging that certain acts are "deceptive" or "unfair." A business commits a "deceptive" practice if it promises that it will keep data secure but then suffers a breach through inadequate safeguards. A business commits an "unfair" practice if it fails to adopt industry-standard security measures. The FTC has not issued any formal regulations defining which practices are unfair, although it has published informal guidance listing the steps businesses should take to protect consumer information (see Sidebar). Some of the conduct it has deemed "unfair" in the past include the failure to set up robust log-in protocols, to protect against "commonly known or reasonably foreseeable attacks from third parties attempting to obtain access to customer information," to encrypt data, and to provide cybersecurity training.

The FTC's suggestions for standard data security practices

In its informal manual, "Protecting Personal Information: A Guide for Business," the FTC identifies practical tips for businesses who handle customer's PII.

The FTC advises that a sound data security plan is built on five key principles:

1. Take stock. Know what personal information you have in your files and on your computers.
2. Scale down. Keep only what you need for your business.
3. Lock it. Protect the information that you keep.
4. Pitch it. Properly dispose of what you no longer need.
5. Plan ahead. Create a plan to respond to security incidents.

Importantly, this advice is not just for big businesses. "Some of the most effective security measures — using strong passwords, locking up sensitive paperwork, training your staff, etc. — will cost you next to nothing and you'll find free or low-cost security tools at nonprofit websites dedicated to data security. Furthermore, it's cheaper in the long run to invest in better data security than to lose the goodwill of your customers, defend yourself in legal actions, and face other possible consequences of a data breach." One hard-won insight: don't use email to send sensitive customer information internally. Regular email is not secure. Instead, use encrypted transmissions to send such information, even when the communication is in-house.

Section 5 does not give the FTC fining authority. Thus, FTC enforcement actions typically result in consent decrees that prohibit the company from future misconduct and require audits for up to 20 years. However, the FTC is able to fine businesses that have violated a consent decree. For example, in August 2012 Google agreed to pay the FTC $22.5 million to settle charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC.

Even if the FTC does not impose a fine, FTC scrutiny can trigger follow-on class action litigation, as illustrated by the case of CBR Systems. In December 2010, a thief stole a company laptop and other electronic storage devices holding the unencrypted PII of about 300,000 CBR clients. The FTC opened an investigation into whether CBR had engaged in deceptive practices by failing to protect its customers' personal data. The FTC eventually filed a complaint, and CBR entered into a 20-year FTC consent order. Meanwhile, CBR customers filed a putative class action under California privacy and unfair competition law. The case settled in February 2013 after a motion to dismiss was filed, with CBR agreeing to reimburse affected clients for identity theft-related losses, pay for class members' two-year subscription to a credit monitoring program (worth $112 million), and pay $600,000 in attorneys' fees.

State regulations

Without any overarching federal regime, state laws are currently the primary source of cybersecurity regulation. While each state's law is slightly different, California provides a good rule-of-thumb because it has one of the strictest privacy regimes and other states use California as a template for their own laws. Thus, this analysis will focus on California's regulations, which can be ultimately summarized in five simple requirements (see the sidebar for a brief overview of Massachusetts' law for comparison).

Massachusetts Data Security Law

The attorney general, director of consumer affairs and business regulation, must be notified regarding a breach. Massachusetts consumers may seek damages under Chapter 93A, which allows for certain instances of treble damages. No notice is required as long as the data acquired or used is encrypted, and the confidential process or key that is capable of compromising the security, confidentiality or integrity of personal information has not been acquired.

While California has one of the most ubiquitous data privacy regimes, Massachusetts' 201 C.M.R. 17.00 (Standards for the Protection of Personal Information of Residents of the Commonwealth) is generally considered the most onerous. Notably, 201 C.M.R. 17.00 requires any business that owns or licenses the PII of Massachusetts residents to implement a written information security program ("WISP") with appropriate administrative, technical and physical safeguards. This goes far beyond other states' data breach disclosure laws which deal with the consequences of lost or stolen data, but don't require preventative protection programs or delineate what those programs should include. For example, California, like many other states, merely requires businesses to implement "reasonable security measures," but does not define what those measures might be. 201 C.M.R. 17.00, on the other hand, details the specific elements that each business's information security program should contain (although the scope of each element is adjusted according to the size and

resources of the business), and requires that PII be encrypted when stored on portable devices, or transmitted wirelessly or on public networks. In the event of a possible compromise, companies must be prepared to produce evidence of a compliant WISP to avoid penalties.

First, California has a *"privacy policy"* statute called the Online Privacy Protection Act of 2003 (CalOppA). Under CalOppA, a commercial website operator that collects PII must "conspicuously post its privacy policy on its Web site." If your privacy policy falls short, you will receive a notice of non-compliance giving you 30 days to fix your website before you are subject to legal action.

Second, California has an *"opt in or out"* statute called the Shine the Light law. Under the Shine the Light law, if your company shares a customer's PII with third parties for direct marketing purposes, you must allow customers to either opt-in or opt-out, and provide additional information about the sharing upon request.

Third, California has a law that requires businesses to implement *"reasonable security measures,"* called the Data Safeguard Law. Under this law, if your company owns, licenses, or maintains a customer's PII, you must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

Fourth, California has a *"data breach notification"* law called, appropriately, the Data Breach Notification Law." Under this law, if your company is the subject of a cyber-attack, you must notify any California resident whose unencrypted PII was acquired, or reasonably believed to have been acquired, by an unauthorized person. You must complete notification in the most expedient time possible and without unreasonable delay. You must offer free identity theft prevention and mitigation services to consumers for at least a year if their Social Security or driver's license number was compromised. If the breach involved more than 500 California residents, you must also notify the California attorney general.

Fifth, there are California laws that impose *additional requirements upon particular kinds of PII.* For example, California's Song-Beverly Credit Card Act restricts businesses from requesting, or requiring, as a condition to accepting credit card payments, PII such as the cardholder's address, telephone number or zip code.

Taken as a whole, state regulations require:

- A conspicuous privacy policy;
- Consumer consent for sharing PII with third-parties;
- Reasonable security measures;
- Notification in the event of breach; and
- Additional protections for highly sensitive kinds of information.

Attorneys general around the country are actively enforcing state data privacy laws. For example, California Attorney General Kamala Harris sued Kaiser for taking six months to notify consumers about a data breach due to a lost external hard drive that inadvertently turned up at a thrift store. Although Kaiser's internal investigation was ongoing, Harris said that the delay was "unreasonable" and sued Kaiser for $2,500 for each violation — which could have added up to a $51.3 million fine.

The case eventually settled for $150,000.

Consumer class action litigation

Government agencies are not the only threat. Where there is a cybersecurity breach, there is a plaintiff's lawyer. In fact, according to one report, Target was hit with over 40 different lawsuits within the first 10 days of going public with its massive security breach back in December 2013.

Data privacy litigation raises a diverse mix of claims under both federal and state law. Thus far, most have been dismissed in the early stages due to lack of standing or failure to state a claim. But those that have made it past the motion to dismiss stage have settled for sizeable sums. The following section reviews the most common claims, issues and outcomes.

Common claims

Consumers can bring actions under a diverse mix of federal and state laws. Some of the common federal claims include those brought under: (1) the Wiretap Act, which prohibits the unauthorized intentional access or disclosure of an intercepted communication; (2) the Stored Communications Act, which prohibits the unauthorized intentional access or disclosure of a stored communication; and (3) the Computer Fraud and Abuse Act, which prohibits the unauthorized accessing of a "protected" computer with the intent to obtain information, further a fraud, or damage the computer or its data ($5,000 minimum damages requirement). Of course, a plaintiff may also seek federal jurisdiction under the Class Action Fairness Act (CAFA), which permits jurisdiction where more than two-thirds of the members of the putative class are alleged to be citizens of states other than that of the named plaintiff and the amount of damages alleged exceeds $5 million dollars.

Some common state claims include: (1) violations of state data privacy regulations (such as CalOppa, or the Shine the Light law); (2) violations of consumer protection statutes (e.g., California Legal Remedies Act, which provides a potential remedy to consumers for damages in connection with a consumer transaction, or the Unfair Competition Law); (3) constitutional violation of right to privacy; and (4) common law claims such as breach of contract, false advertising, negligence, unfair competition, unjust enrichment, trespass, conversion, fraudulent or negligent misrepresentation, public disclosure of private facts, and actual and constructive fraud.

First line of defense: Arbitration clause

Recent Supreme Court decisions have upheld arbitrations clauses requiring consumers to bring claims only in individual arbitrations, rather than in court as part of a class action. While this precedent would seem to suggest that companies should employ such clauses as a first line of defense against massive data breach class action lawsuits, many companies have run into hurdles attempting to get these clauses enforced.

For example, Zappos attempted to argue that an arbitration provision included in its Terms of Use policy should block a data breach class action. The court disagreed, finding that the agreement was not enforceable because it was a "browse-wrap" agreement (an agreement that purports to bind users simply because they browsed the website) that was only accessible via a "highly inconspicuous hyperlink buried among a sea of links." Thus, the court could not "conclude that Plaintiffs ever viewed, let alone manifested assent to, the Terms of Use."

Similarly, the Ninth Circuit declined to enforce Barnes & Noble Inc.'s "browse-wrap" terms of use agreement, including an arbitration provision, against a plaintiff customer. The court held that plaintiff did not affirmatively assent to those terms because there was no evidence that he had actual notice of them. Although Barnes & Noble did make its terms available via a conspicuous hyperlink on every page of its website, it did not require users to take any affirmative action to demonstrate assent.

In contrast, courts have upheld online arbitration provisions where they are conspicuously displayed or where they require affirmative consent. Affirmative consent can be obtained by requiring users to actively click on a button "agreeing" to a website's terms of service, including its arbitration clause.

Second line of defense: Lack of standing

The most common and successful defense to data privacy class actions is clear: Article III standing due to lack of "injury in fact." While then-Judge Alito has argued that "[i]njury-in-fact is not Mount Everest," a recent California district court dubbed it the "Kilimanjaro" of data privacy cases.

Standing requires a plaintiff to show that he or she has a personal stake in the litigation. This includes alleging an "injury-in-fact" that is both "concrete and particularized" and "actual or imminent." Although it concerned government surveillance, the seminal case regarding standing in the data-privacy arena is the 2013 case of *Clapper v. Amnesty International USA.* In *Clapper*, the plaintiffs claimed that the US government's increased surveillance measures forced them to spend more money securing their overseas communications. The Supreme Court found that "the claims of the challengers that they were likely to be targets of surveillance were based too much on speculation and on a predicted chain of events that might never occur." Thus, plaintiffs failed to establish standing because their alleged future injuries-in-fact were not "certainly impending." The Court also rejected the plaintiffs' standing argument based on the expenses and inconvenience they incurred to protect themselves against future harm. Plaintiffs could not "manufacture" standing "merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."

Pre-*Clapper* there were a few cases where courts found standing despite lack of any damages or cognizable harm. Since *Clapper* was decided over two years ago, it has shut down the majority of would-be cybersecurity class actions. For example, in *In re Barnes & Noble Pin Pad Litigation*, the court dismissed a putative consumer class action based on hacked PIN pad devices in the Barnes & Noble stores, finding no evidence of any certainly impending future injury. Only one plaintiff suffered from actual fraudulent activity, but the charge was canceled by her credit card company. Likewise, in *Remijas v. Neiman Marcus Group, LLC*, hackers breached Neiman Marcus' computer network, resulting in the potential disclosure of 350,000 customers' payment card data and PII. The court found that plaintiffs lacked standing despite the intentional hack because the alleged harm was speculative, and because plaintiffs were reimbursed for any actual fraudulent charges by their credit card companies.

Litigation by banks

For now, the real litigation danger may not come from consumer class-action litigation. Rather, it may come from lawsuits brought by banks alleging massive injuries from processing fraudulent charge-backs after security breaches. Standing is not an issue in these cases because the banks can show actual damages. In two of the largest data breach settlements, TJ Maxx settled with Visa for $40 million in 2007 after a breach involving an estimated 100 million credit and debit cards, while

Heartland Payments Systems settled with Visa for a whopping $60 million in 2010 after a breach involving an estimated 130 million credit and debit cards.

Target also recently settled with several credit card companies after its massive data breach involving an estimated 40 million accounts. The court denied Target's motion to dismiss, finding that the banks had adequately pled actual damages. The court also found that Target owed a duty of care to the issuer banks with regard to its data security practices, and that the breach was foreseeable because Target had deliberately disabled one of the security features that could have prevented the harm. Target recently settled with Mastercard for $19 million, and is continuing to negotiate with Visa.

While the banks currently seem to be focusing on massive data breaches, this is an area for any business that processes credit cards to watch. Contact your credit card processor to determine what security measures they might require ahead of time, instead of waiting for them to inform you via a filed complaint that they consider your measures inadequate.

However, *Clapper* has not totally shut down data privacy class actions. In California, there are two notable cases. In *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, Judge Koh found injury because plaintiffs' information was stolen and wrongfully disseminated, even though no misuse occurred. Sony eventually settled the case for $17.5 million ($15 million in damages, and $2.5 million in attorney fees). Likewise, in *In re Adobe Sys. Privacy Litig.*, Judge Koh found standing in a case where hackers specifically targeted and definitely stole plaintiffs' personal data. The judge found that "the threatened injury here could be more imminent only if plaintiffs could allege that their stolen personal information had already been misused." This case is still being litigated.

A Minnesota district court judge reached a similar conclusion in *In re Target Corp. Customer Data Sec. Breach Litig.* In that case, 40 million credit cards were compromised in the breach during the 2013 holiday shopping season. Plaintiffs alleged that they suffered "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees." The judge rejected Target's lack of standing argument, finding that plaintiffs had pled actual damages. The judge also found that they had pled certainly impending injury due to a substantially increased risk of future fraud. The judge distinguished *Clapper* because plaintiffs in that case were not certain whether their communications were going to be monitored, whereas the plaintiffs in *In re Target* demonstrated that a data breach had in fact occurred. On March 19, 2015, Target agreed to pay $10 million to settle the lawsuit.

In addition, some plaintiffs have established standing by alleging that they paid additional money to a company in exchange for a premium policy that included data security protection. In *In re LinkedIn User Privacy Litig.*, the plaintiff alleged that she paid for LinkedIn's premium subscription in reliance on LinkedIn's Privacy Policy, which had stated that LinkedIn had adequate security procedures. She asserted that LinkedIn's failure to adhere to industry standards and its privacy policy caused the breach that revealed her password. The plaintiff's allegation that she would not have purchased a premium subscription without the promised security procedures was sufficient to confer standing under both Article III and California's UCL. LinkedIn has since agreed to pay $1.25 million to settle this case.

The settlements in these cases demonstrate that standing is a major obstacle. However, if plaintiffs' lawyers can make it past the dismissal stage, there is the potential of large payouts. The fact that

some cases have survived and enjoyed hefty payouts ensures that this type of litigation will continue unabated.

Third line of defense: Failure to state a claim, unverifiable class

Even if plaintiffs manage to get past Article III standing issues, there are still many ways to defeat these actions. Many flounder at the motion to dismiss stage for failure to plead a cognizable injury or other essential facts. In *In re iPhone Application Litig.*, for example, Judge Koh found that allegations that defendants violated the Wiretap Act and Stored Communications Act were sufficient to confer statutory standing (see sidebar). She also upheld standing on other grounds despite *Clapper*, including detrimental reliance on Apple's privacy policy. Ultimately, however, she dismissed most claims for failure to state a claim, including those under Stored Communications Act, Wiretap Act, CAFA, California Constitution and various common law state law claims.

Statutory standing

Ever-creative plaintiffs' lawyers may have found an alternative work-around to Clapper: statutory standing. The Ninth Circuit and some other district courts have found that injury to statutory rights can create Article III standing even without actual damages. It has reasoned that "a concrete injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." See Jewel v. NSA, 673 F.3d 902, 908 (9th Cir. 2011); Edwards v. First Am. Corp., 610 F.3d 514, 515-17 (9th Cir. 2010), cert granted 131 S. Ct. 3022 (2011), dismissed (June 28, 2012) (same).

Like the few cases that found standing under Clapper, cases where courts find statutory standing also demonstrate the potential for hefty payouts. In Harris v. comScore, 292 F.R.D. 579 (N.D. Ill. 2013), web users sued comScore for allegedly installing data-harvesting software on their computers without consent and selling that information to third-parties. In a rare victory, the court found that statutory damages were a sufficient basis for standing. It also found that such damages eliminated the need for plaintiffs to prove their injuries individually and certified a class. The Seventh Circuit denied the appeal, and the case recently settled for $14 million.

Whether or not statutory standing is a viable alternative to Clapper may soon be decided. The Supreme Court recently granted cert in a data privacy case, Robins v. Spokeo Inc., No. 13-1339 (June 9, 2014), in which statutory standing is at issue. In Spokeo, the Ninth Circuit held that the plaintiff could adequately plead Article III standing despite lack of actual harm by alleging a claim for a willful violation of the Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681). If the Supreme Court supports the Ninth Circuit's analysis, Spokeo may well turn out to be the important privacy class action and consumer case of the decade.

Others flounder at the class certification stage. Some common certification hurdles include a finding that a class is unascertainable because no records exist, or a finding that injury would require individualized inquiries into each consumer's evidence of identity theft. For example, in *In re Hulu Privacy Litig.*, the court found that the customers of online video content provider Hulu LLC successfully demonstrated injury under the Video Privacy Protection Act by alleging that the company wrongfully disclosed their personal information to third parties. However, the court ultimately denied

class certification due to lack of ascertainability because the violations wouldn't affect the Hulu users who took measures to prevent the tracking of their personal data.

Ten ways to minimize your litigation risk

This legal overview provides some important takeaways regarding cybersecurity litigation. Here are 10 basic measures any company can take to minimize its risk at every step of this process:

1. Make sure that your privacy policies are complete and accurate. You must disclose whether you store, track or disclose your customer's PII, and allow customers to opt in or out of this collection. That includes data that you allow third parties to store, track or collect. An inaccurate privacy policy is a simple way to get plaintiffs past the motion to dismiss stage, or to give the FTC grounds
   to allege that you are employing "deceptive" practices under Section 5 of the FTC Act.
2. Along with your "conspicuous" privacy policy, include a "conspicuous" arbitration clause covering any data breach claims. The best practice is to require affirmative consent to its terms.
3. Consider whether your privacy policy or any other consumer contract states or implies that consumers are paying for data protection. You may want to remove any such express or implied promise. This simple contractual benefit may be enough to get a consumer class action past the motion to dismiss stage and into costly settlement discussions.
4. Think simple. Ensure that sensitive customer data is not stored on any laptops or other storage devices. Many expensive cases have their humble beginnings when this hardware is inadvertently left somewhere or stolen.
5. Investigate industry practices to ensure that you are employing "reasonable security measures" to protect consumer's data privacy under state law, and that you are not employing "unfair" practices under Section 5 of the FTC Act. In the event of litigation, what affirmative steps will your company point to as evidence that you were employing adequate security measures? Set up multiple electronic safeguards, including robust log-in protocols; firewalls to prevent outside attacks; data encryption; endpoint protection, intrusion detection, data retention policies that employ regular deletion of PII and other information that is no longer needed; backing up data information to determine the extent of a breach if one occurs; and providing cybersecurity training to key employees.
6. Gain additional protection by making sure you get favorable indemnification clauses and liability waivers with third-party vendors who supply software or online platforms. Don't be liable for their data weaknesses.
7. To avoid plaintiffs taking advantage of the favorable post-*Clapper* precedent in California, consider including a choice of law clause in any consumer contracts (written or electronic) that ensures California law does not apply.
8. Ensure that you have a notification plan in place in the event of a breach. If you wait until after a breach occurs to devise a plan, you are at risk for regulatory and civil action alleging that you took an unreasonably long time to notify consumers.
9. Offer to reimburse affected consumers for any identity-theft related losses and pay for a credit-monitoring program. This offer both eases public relations and ensures that plaintiff's lawyers cannot use those expenditures as a basis for standing.
10. Ensure that any lawyer you hire to work on your case is well-versed in the latest case law, and is prepared to file an aggressive motion to dismiss plaintiffs' claims based on lack of standing and lack of cognizable injury.

Further Reading

For ease of reference, we use the term PII to refer to any form of personally identifiable information. Note, however, that PII may be defined differently under different statutes.

15 U.S.C. §§ 6501 et seq.

42 U.S.C § 201 et. seq.

15 USC § 1681 et seq.

15 U.S.C. § 45.

FTC, Protecting Personal Information: A Guide for Business.

See In re CBR Systems, Inc., FTC File No. 112 3120 (2013).

Johansson-Dohrmann v. Cbr Systems, Inc., No. 12-cv-1115-MMA (BGS), 2013 WL 3864341 (S.D. Cal. July 24, 2013); see also LaCroix, “Cybersecurity Enforcement: The FTC Is Out There” (supra n. 7).

CA Bus. & Prof. Code §22575.

Cal. Civ. Code Sections 1798.80-84

Cal. Civil Code Section 1798.81.5

California Civil Code Section 1798.82

Cal. Civ. Code Section 1747 et seq.

AT&T Mobility LLC v. Concepcion, 563 U.S. __, 131 S. Ct. 1740, 1752 (2011) (state claims); American Express Co. v. Italian Colors Restaurant, 133 S. Ct. 2304, 2307, 2309 (2013) (federal claims).

In re Zappos.com, Inc., Customer Data Security Breach Litigation, 893 F. Supp. 2d 1058 (D. Nev. 2012).

See, e.g., Nguyen v. Barnes & Noble Inc., No. 12–56628, (9th Cir. Aug. 18, 2014) (upheld because terms were conspicuous).

PDC Labs. Inc. v. Hach Co., No. 09- 1110, (C.D. Ill. Aug. 25, 2009).

Citing to federal caselaw, state courts have also found that plaintiffs alleging future injury due to data breach lack standing under state law. See, e.g., Vides v. Advocate Health & Hosps. Corp., No. 13-CH-2701 (Ill. 19th Judicial Cir. May 27, 2014); Maglio v. Advocate Health & Hosps. Corp., No. 13-CH-2701 (Ill. 16th Judicial Cir. July 10, 2014); Heller v. Ralphs Grocery Co., No. B249608 (June 23, 2014).

Danvers Motor Co. v. Ford Motor Co., 432 F.3d 286, 294 (3d Cir. 2005).

In Re Google, Inc. Privacy Policy Litigation, C-12-01382-PSG, (N.D. Cal., Dec. 3, 2013).

Lujan v. Defenders of Wildlife, 112 S. Ct. 2130, 2136 (1992).

133 S. Ct. 1138 (2013).

See, e.g., Pisciotta v. Old National Bancorp., 499 F.3d 629 (7th Cir. 2007) (finding standing based on the threat of future harm from an intrusion that was “sophisticated, intentional and malicious”); Resnick v. AvMed, Inc. 693 F.3d 1317 (11th Cir. 2012) (finding standing because the laptop containing plaintiffs’ PII was actually stolen, even though plaintiffs did not show any actual misuse of their identity).

Case # 12-cv-8617 (N.D.Ill. Sept. 3, 2013).

2014 U.S. Dist. LEXIS 129574 (N.D. Ill. Sept. 16, 2014)

MDL 11MD2258 AJB MDD, 2014 WL 223677 (S.D. Cal. Jan. 21, 2014)

2014 U.S. Dist. LEXIS 124126 (N.D. Cal. Sept. 4, 2014).

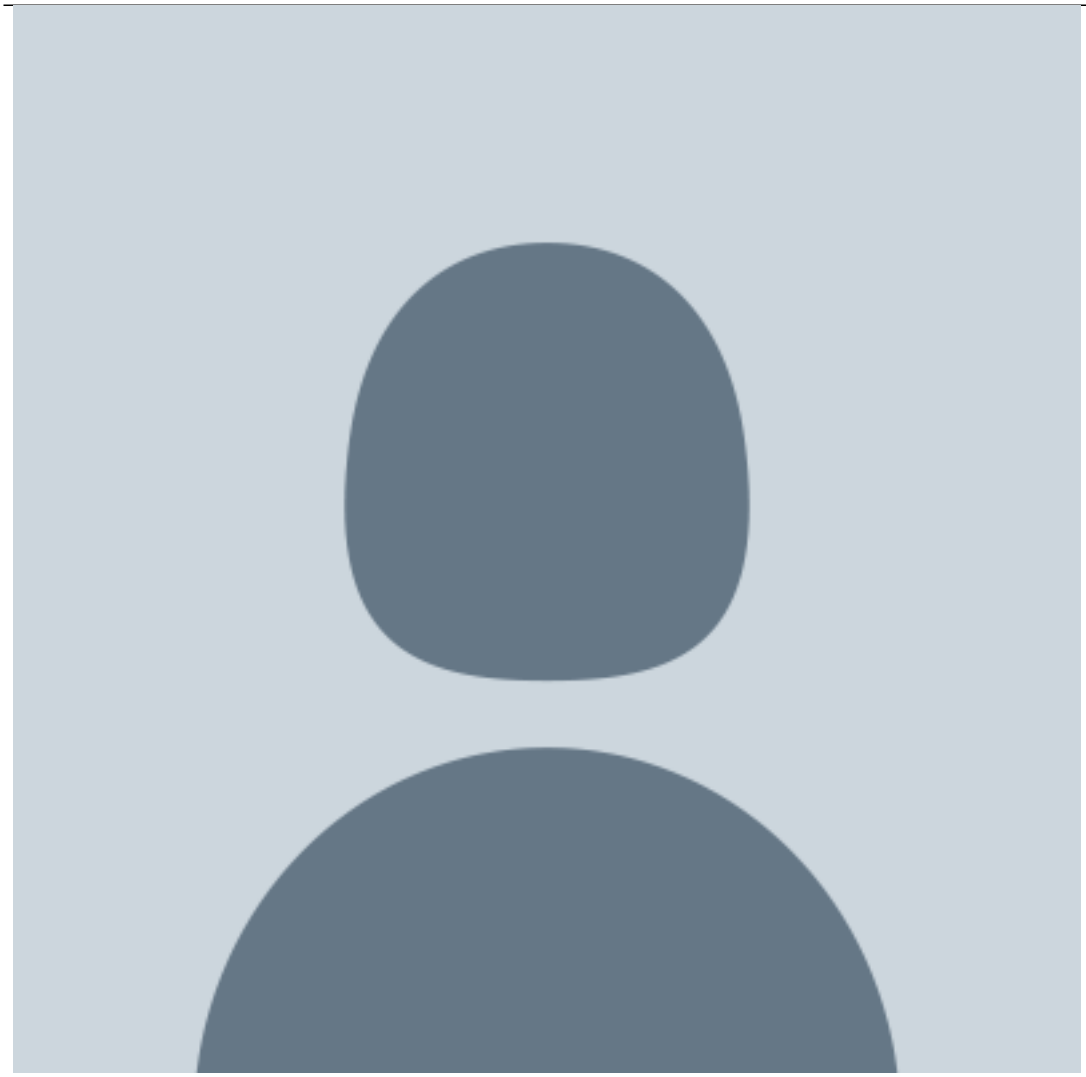
No. MDL 14-2522, 2014 WL 7192478, at *2 (D. Minn. Dec. 18, 2014).

No. 5:12-CV-03088-EJD, 2014 U.S. Dist. LEXIS 42696, at *11 (N.D. Cal. Mar. 28, 2014).

11-MD-02250-LHK (N.D. Cal.; Jun. 12, 2012).

No. C 11-03764 LB, 2012 WL 2119193, at *8 (N.D. Cal. Jun. 11, 2012).

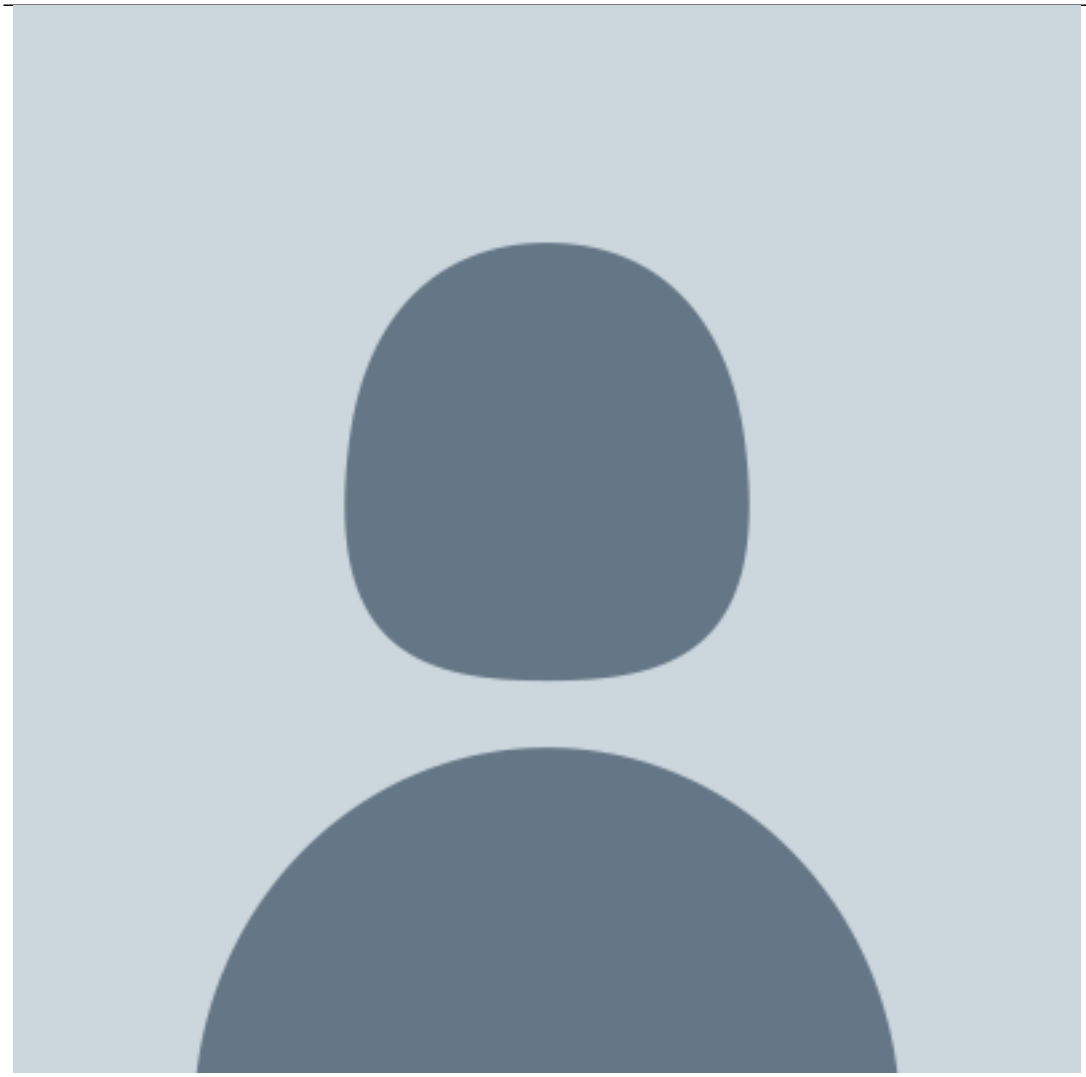
Todd H. Greene



Senior Vice President and General Counsel

Penske Media Corp

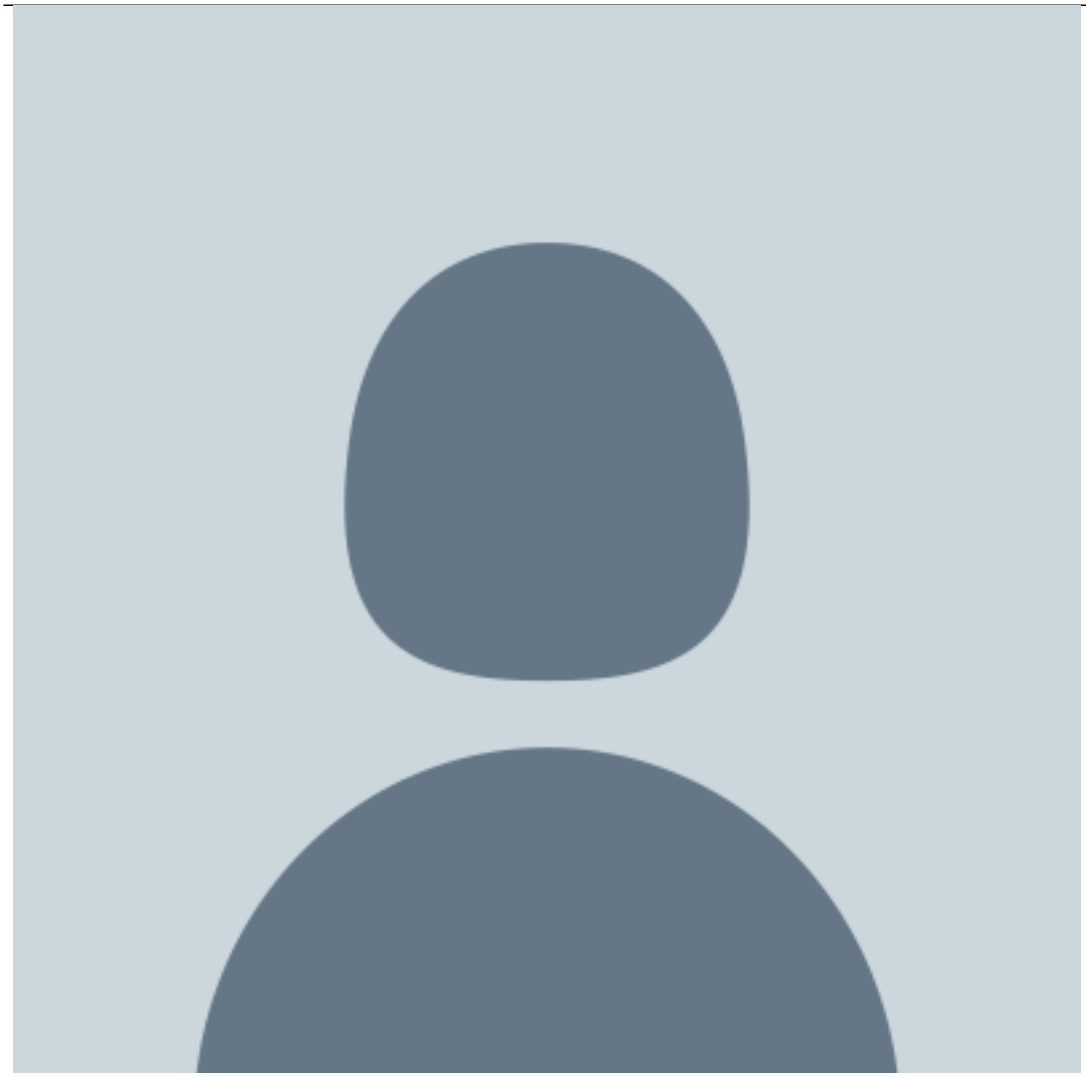
William A. Delgado



Partner

Willenken, Wilson, Loh & Delgado LLP

Nicole A. Diaz



Senior Associate

Willenken, Wilson, Loh & Delgado LLP