SIDLEY AUSTIN LLP
SIDLEY

The Last Year in Privacy & Security Litigation; Government Access to Private Sector Data
Select Cases from January 1, 2014 to February 28, 2015

Alan Charles Raul[1]
Adam Farra
SIDLEY AUSTIN LLP

March 2015

Executive Summary

A few key takeaways shape the contours of litigation in these areas over the past 14 months.

- **Courts are easing up somewhat on plaintiffs regarding Article III standing, but hard questions remain and the Supreme Court's involvement is possible.**

    - For federal and state statutory claims, more courts are finding that a violation of a privacy/data security statute is enough to satisfy Article III. No individual harm needs to be alleged.

        - ***Some inside baseball.*** We will probably have a Supreme Court case resolving that tricky issue in the next two years. The Court has called for the views of the Solicitor General in a Ninth Circuit case that raises this question (O'Scannlain wrote the opinion in *Spokeo*), suggesting that it is well-aware of the importance of this issue. The Court's starkly pro-privacy decision in the 2014 cellphone case (*Riley*) was also a highly significant development.

    - For common law claims, the courts are more stringent, but seem to be more open to accepting plaintiffs' arguments that misappropriation of information is an Article III injury because that information *has a marketplace value*. That is different than the older misappropriation theories for injury, which rested more heavily on the violation of an individual's reasonable expectation of privacy.

    - Finally, courts continue to be split over whether increased risk of identity theft and incurred costs for data protection are enough to satisfy Article III. The cases seem to turn on magnitude, *i.e.*, the more serious the breach (and the bigger the press attention), the more likely a court is going to accept that a data breach has created a sufficiently high risk of future data theft for Article III purposes.

[1] Alan Charles Raul is a partner in Sidley's DC office and lead global coordinator of the firm's Privacy, Data Security and Information Law group. Adam Farra is an associate in Sidley's DC office.

- **Most privacy litigation, whether common law or statutory, is faltering on some permutation of three arguments:**

    - (1) Consent by the plaintiff permits the defendant to harvest, share, analyze, and sell that plaintiff's information;

    - (2) The defendant's security and privacy controls were reasonable and sufficient; and

    - (3) Any information misappropriated or shared is not sufficiently sensitive to permit a privacy invasion-related cause of action.

- **The exception is misrepresentation cases.** Courts are relatively more receptive to claims that the defendant's representations about the quality of its data protections were overblown and inconsistent with what was actually available, inducing plaintiffs into relying on those representations to do business with them.

Privacy Litigation

Beyond Systems, Inv. v. Kraft Foods, Inc., --- F.3d ---, 2015 WL 451944 (4th Cir. 2015) (Feb. 4, 2015). [*]

The plaintiff sued Kraft for violations of Maryland and California's anti-spam statutes. Kraft moved for judgment after a jury trial, asserting that Beyond Systems had invited the harm by, among other things, creating fake e-mail accounts to hoard spam and then bouncing that spam between Maryland and California servers in an attempt to magnify the statutory damages. The district court agreed with Kraft, and the Fourth Circuit affirmed, holding that "the common law doctrine of *volenti non fit injuria* precludes Beyond Systems' recovery under the California and Maryland anti-spam statutes."

Locklear v. Dow Jones & Company, No. 14-744 (N.D. Ga. 2015) (Jan. 23, 2015).

Each time the plaintiff viewed a video clip on the Wall Street Journal Live Channel on her Roku, Dow Jones disclosed her Roku device serial number and video viewing history to mDialog, an analytics and advertising company. mDialog, in turn, created individualized user identities relying in part on this information.

The plaintiff sued Dow Jones in a class action for violation of the Video Privacy Protection Act, alleging that the Roku serial number and video viewing history constituted personal identifying information. Dow Jones moved to dismiss the case; the district court granted the motion. Dow Jones first asserted that the plaintiff lacked Article III standing due to lack of an injury. The district court disagreed, concluding that the word "aggrieved" in the Video Privacy Protection Act has a broad meaning and therefore could be satisfied by the plaintiff's allegations. Dow Jones next asserted that the plaintiff was not a "consumer" within the meaning of the Video Privacy Protection Act because she did not pay to watch the WSJ Live Channel; the district court rejected that argument, concluding that no exchange of money is required for a plaintiff to qualify as a subscriber/consumer for purposes of the statute.

Dow Jones also argued that the serial number and video viewing history did not constitute personal identifying information. With this argument, the district court agreed, concluding that because mDialog had to take additional, independent steps to turn the serial number and video viewing history into an individualized user profile, the information did not constitute personal identifying information. On this basis, the district court dismissed the case.

In re Nickelodeon Consumer Privacy Litigation, 2015 WL 248334 (D.N.J. 2015) (Jan. 20, 2015).

In this class action, the plaintiffs – minors under the age of thirteen – claimed that Viacom and Google invaded their privacy when it collected information about them when they registered for profiles on certain kids' websites. Their claims also centered on the allegation that Viacom and Google placed "cookies" on the plaintiffs' computers without their consent, allowing Viacom to

[*] Disclosure: I clerked for the district judge in *Beyond Systems* while the case was ongoing (Judge Messitte).

gather information about the minor plaintiffs. The plaintiffs asserted Video Privacy Protection Act and New Jersey Computer Related Offenses Act claims, as well as intrusion upon seclusion. The defendants moved to dismiss the case.

The district court dismissed the Video Privacy Protection Act claim because the data the defendants collected – IP addresses, in particular – did not identify individual persons and therefore could not be tied to a plaintiff's video watching habits. The district court dismissed the New Jersey Computer Related Offenses Act claim, ruling that the plaintiffs had failed to allege any business or property damage arising out of the defendants' conduct. The district court also dismissed the intrusion upon seclusion claim, concluding that the plaintiffs failed to allege facts sufficient to satisfy the "highly offensive" prong of the tort. In particular, it concluded that the case law set the "highly offensive" standard quite high, preventing the plaintiffs from making out a claim based on the collection of information about minors.

Campbell v. Facebook, Inc., -- F. Supp. 3d --, 2014 WL 7336475 (N.D. Cal. 2014) (Dec. 23, 2014).

Facebook provides a messaging service to its users. The plaintiffs alleged that Facebook would scan their private messages to assess whether there was a link to a web page contained in the message; if so, Facebook counted the reference as a "like," and it used that data to create user profiles to deliver targeted advertising. The plaintiffs alleged that Facebook's scans of the messages violated the Electronic Communications Privacy Act, California's Invasion of Privacy Act, and California's unfair competition law. Facebook moved to dismiss the claim. The district court dismissed the state claims but allowed the federal claim to proceed.

With respect to the federal claim, Facebook argued that its scanning of the messages fell into the statutory exception permitting electronic communications service providers to intercept communications occurring in "the ordinary course of [their] business." The district court disagreed, eschewing a categorical approach to defining "ordinary course of business" and instead applying "the ordinary course of business" exception to the particulars of *Facebook*'s business. Facebook did not provide any details explaining the ordinary course of its business, and the district court rejected "the suggestion that any activity that generates revenue for a company should be considered within the 'ordinary course of its business.'" Facebook also argued that the plaintiffs consented to the interception of their messages; the district court rejected that argument, concluding that the disclosures were insufficiently specific because they did not mention "the scanning of message content *for use in targeted advertising*." (Emphasis added.)

The court dismissed the state claims. It dismissed the California Invasion of Privacy Act claim, citing California state court cases holding that internet communications are not "confidential" within the meaning of that Act "because such communications can easily be shared by, for instance, the recipient(s) of the communications." The court dismissed the California unfair competition claim, holding that the plaintiffs failed to establish statutory standing. In particular, the court held that the plaintiffs failed to allege that they "lost any money or property as a result

of Facebook's conduct." It rejected the argument that the plaintiffs' property interest in their personal information was sufficient to satisfy statutory standing.

Backhaut v. Apple, Inc., -- F. Supp. 3d –, 2014 WL 6601776 (N.D. Cal. 2014) (Nov. 19, 2014).

The plaintiffs in this class action sued Apple for violations of the Stored Communications Act, the Wiretap Act, California's unfair competition law, and California's Consumers Legal Remedies Act. The core allegation was that Apple prevents "former Apple device users from receiving text messages sent to them from current Apple device users." In particular, when a former iPhone user switches to a non-Apple device, the user has great difficulty receiving text messages from iPhone users. The difficulty appears to be because iMessage, Apple's messaging system, bypasses the SMS/MMS text messaging systems. Apple moved to dismiss the case; the court dismissed the claims without prejudice.

The district court dismissed the Stored Communications Act claim because there were no allegations that Apple accessed *stored* communications. There were no allegations that Apple accessed "a facility through which an electronic communication service is provided," or that it accessed or intercepted the text messages while they were in electronic storage.

With respect to the state law claims based on Apple's misrepresentations and/or fraud, the district court ruled that the plaintiffs lacked standing to pursue their claims because they failed to allege that Apple's interception of their messages affected the functionality of their new phones, or that they overpaid for their Apple devices *in reliance upon* Apple's representations regarding interception of messages.

The district court declined to dismiss the Wiretap Act claim. It held that the complaint sufficiently alleged that Apple had intentionally intercepted text messages sent from current Apple device users to former Apple device users. It rejected Apple's argument that the plaintiffs consented to the interception; the software license, the court held, was not sufficiently specific to place the user on notice that Apple would "intercept his or her messages when doing so would not 'facilitate delivery' of the messages." With respect to the state law claims based on unfair business practice, the court sustained those claims that were derivative of the Wiretap Act, but dismissed the claims based on fraud, concluding that the facts were insufficient to conclude that Apple intentionally deceived its users.

Sterk v. Redbox Automated Retail LLC, 770 F.3d 618 (7th Cir. 2014) (Oct. 23, 2014).

Redbox provides a third-party with access to its customer database so that the third-party may field customer inquiries and address customer service issues. The plaintiffs sued Redbox, alleging that the disclosure of their information to the third-party violated the Video Privacy Protection Act. The district court granted summary judgment to Redbox, concluding that the disclosures were in the ordinary course of its business because they were incident to "request processing," thereby falling into a statutory liability exemption. The Seventh Circuit agreed, holding as a matter of statutory construction that "request processing" includes customer service requests, thereby permitting Redbox to share customers' information with the third-party it hired

to address customer inquiries. Separately, the Seventh Circuit rejected Redbox's argument that the plaintiffs lacked standing, concluding that statutory injury need not require pecuniary loss for a plaintiff to have standing.

In re Google, Inc. Privacy Policy Litigation, -- F. Supp. 2d –, 2014 WL 3707508 (N.D. Cal. 2014) (July 21, 2014).

Google collects information through its various products and uses that information to place advertisements tailored to each consumer. For several years, Google's policies regarding whether it could commingle the information it collects through its various products was uncertain; in 2012, Google unified its policy in favor of commingling such information.

The plaintiffs sued Google for moving to this less-protective privacy policy without the user's consent, alleging that the new policy violates California's Consumers Legal Remedies Act, the federal Wiretap Act, the Stored Electronic Communications Act, California's unfair competition law, and constitutes a breach of Google's old contract terms with its users. The plaintiffs also alleged intrusion upon seclusion. Google moved to dismiss the claims, and the district court mostly agreed with it.

With respect to standing, the court dismissed the plaintiffs' claims that Google's less restrictive privacy policy would lead to increased risk of inadvertent disclosure, ruling that this was insufficient to confer Article III standing. The court concluded, on the other claims, that Article III standing was met because of the plaintiffs' allegations that (1) Google's transmission of information drained the plaintiffs' products' battery life, and (2) the plaintiffs' incurred costs in purchasing new products out of privacy concerns.

The court dismissed the Consumers Legal Remedies Act claim because the plaintiffs did not allege that they even saw the privacy policy on which they allegedly relied. The court dismissed the unfair competition law claim because "the disclosure of common, basic digital information to third parties" is not a "serious or egregious violation[] of social norms," and therefore cannot give rise to a cause of action. The court dismissed the intrusion upon seclusion claim for a similar reason – that the intrusion through transmission of this information was not highly offensive to a reasonable person.

Two claims survived: (1) a California unfair competition law claim premised on the allegation that Google held out its privacy policy for its application users knowing that they would falsely believe that their data would be accessed by a limited number of groups; and (2) a breach of contract claim that Google divulged information in violation of the contracts it had with specific application users. (These were admittedly a bit unclear to me.)

Perkins v. LinkedIn Corp., -- F. Supp. 2d –, 2014 WL 2751053 (N.D. Cal. 2014) (June 12, 2014).

LinkedIn harvests email addresses from the contact lists of email accounts associated with LinkedIn members. It then sends invitations to join LinkedIn to those harvested email addresses. The plaintiffs sued LinkedIn for: (1) violation of the common law right of publicity; (2) violation

of California's unfair competition law; (3) violation of the Stored Communications Act; (4) violation of the Wiretap Act; and (5) violation of California's Comprehensive Data Access and Fraud Act. LinkedIn moved to dismiss all of the claims for lack of standing and failure to state a claim.

With respect to standing, the court agreed with the plaintiffs, ruling that use of a plaintiff's name for personalized/targeted marketing purposes has concrete value, and that misappropriation of such information can therefore constitute an injury to a plaintiff.

With respect to failure to state a claim, the court dismissed the federal claims, concluding that the plaintiffs had consented and authorized LinkedIn to use their information – a conclusion that it drew from reviewing LinkedIn's notifications as the consumer makes his or her way through the website. With respect to the right of publicity claim, the court denied the motion to dismiss with respect to the *continued* invitations/"endorsement" emails, but concluded that the *first* invitation or "endorsement" email was consented to by the plaintiffs and therefore had to be dismissed. The court dismissed the Comprehensive Data Access and Fraud Act because the plaintiffs did not allege a harm arising out of LinkedIn's decision to harvest a user's contact list without asking for a password to access that list (the gmail account was open, allowing LinkedIn to get that information without need for the gmail account password). The court granted the plaintiffs leave to amend their complaint to rehabilitate the dismissed portions of their complaint.

Sinibaldi v. Redbox Automated Retail LLC, 754 F.3d 703 (9th Cir. 2014) (June 6, 2014).

Redbox requires users to provide their zip code when they pay to rent movies. The plaintiffs sued Redbox, alleging that the zip code requirement violates California's Song-Beverly Credit Card Act. The district court dismissed the case, concluding that these transactions do not fall within the scope of the statute. The Ninth Circuit affirmed, but on a different ground: That the statute permits collection of personal information in connection with a credit card transaction if the credit transaction is used as a deposit to secure payment in the event of default, loss, damage, or a similar incident. Because the consumer only pays a fee for renting a movie for one day, the credit card secures the movie against a longer period of rental, being lost, destroyed, etc. Thus, the Ninth Circuit concluded that the transaction was for a deposit and affirmed the dismissal. Judge Reinhardt dissented, arguing that the transaction is to fulfill the primary agreement to pay Redbox to rent the movie and not security.

In re Zynga Privacy Litigation, 750 F.3d 1098 (9th Cir. 2014) (May 8, 2014).

The plaintiffs sued Facebook and Zynga for violations of the Wiretap Act and the Stored Communications Act, alleging those entities disclosed confidential user information to third-parties and advertisers. Facebook and Zynga moved to dismiss the claims; the district court granted their motions. The Ninth Circuit affirmed, holding that the claims failed because the plaintiffs did not allege that the defendants disclosed "the contents" of a communication to a third party, rather than disclosing merely customer record information like name, address, or subscriber number (the "referer" information). The Ninth Circuit rejected, in a footnote,

Facebook and Zynga's standing arguments, concluding that the statutes created the defendant's duty to the plaintiff and that violation of that statutory duty constitutes an injury.

In re Facebook Privacy Litigation, 572 Fed. App'x 494 (9th Cir. 2014) (May 8, 2014).

The plaintiffs asserted California unfair competition, Consumer Legal Remedies Act, breach of contract, and fraud claims. The district court dismissed the claims, holding that the allegations that (1) information disclosed by Facebook could be used to obtain personal information about the plaintiffs, and (2) dissemination of that information diminished its market value, were insufficient as a matter of law to infer damages. Similarly, the plaintiffs' failure to allege that they lost money or property as a result of Facebook's conduct barred them from pursuing their unfair competition claim. Finally, the district court dismissed the Consumer Legal Remedies Act claim because the plaintiffs failed to allege that they obtained anything from Facebook by purchase or consumer transaction. The Ninth Circuit affirmed the district court's reasoning.

Opperman v. Path, Inc., 2014 WL 1973378 (N.D. Cal. 2014) (May 14, 2014).

The plaintiffs in this class action sued a set of "app" developers for stealing and disseminating the contact information stored on their phones; it also sued Apple for inadequately securing the phones from the intrusion, and for making attendant misrepresentations. They asserted claims for violation of a myriad of state statutes (the California unfair competition law, Consumer Legal Remedies Act, Comprehensive Computer Data Access and Fraud Act, Wiretap/Invasion of Privacy Act, Uniform Fraudulent Transfer Act, and the Texas Wiretap Act and Theft Liability Act), along with the federal Computer Fraud & Abuse Act, and the Electronic Communications Privacy Act. They also asserted all manner of tort claims, including conversion, negligence, products liability, intrusion upon seclusion, and public disclosure of private facts. The defendants moved to dismiss the case.

Apple. The court rejected Apple's standing argument. With respect to causation, the court ruled that it was sufficient that the "Plaintiffs allege[d] that Apple misled them through its advertising and failed to disclose material information, that each Plaintiff relied on these misrepresentations or nondisclosures, and that each Plaintiff overpaid for Apple's products." Further, the court ruled that Apple's violation of state consumer statutes conferred Article III standing with respect to those claims. The court did, however, reject the argument that the plaintiffs had standing by virtue of injury to their property rights in their address books.

Apple contended that the Communications Decency Act precluded all of the plaintiffs' claims not sounding in misrepresentation. The district court disagreed, concluding that Apple – by virtue of publishing iOS Human Interface Guidelines for app developers – had stepped into the role of "information content provider" and therefore was not protected by the Communications Decency Act.

The district court dismissed the misrepresentation claims against Apple, ruling that there was no allegation indicating that the plaintiff *relied* on Apple's representations regarding whether apps could access a phone user's data. The court rejected the plaintiffs' alternative theory of reliance,

that Apple constructed a long-term advertising campaign in which it held itself out as a paragon of safety and reliability. The district court ruled that there was no evidence of the plaintiffs' exposure to Apple's campaign, no evidence alleging with any specificity the length of any such campaign, and no evidence substantiating the content of such campaign. The district court also rejected the plaintiffs' argument that Apple breached its affirmative duty to disclose the vulnerability of its hardware to theft of address books by third-party apps, ruling that there were no facts indicating with sufficient specificity that Apple warranted the safety of its hardware.

The district court dismissed the Computer Data Access and Fraud Act claim against Apple, holding that because the plaintiffs' allegations did not indicate that Apple circumvented technical or code-based barriers to inhibit the plaintiffs' access to their phones, the plaintiffs' could not establish that Apple acted "without permission." The district court similarly dismissed the Computer Data Access and Fraud Act and Computer Fraud and Abuse Act claims against all of the defendants for the same reason.

The App Developers. Except for the invasion of privacy claim, the district court dismissed the plaintiffs' common law claims against the App Developers on standing grounds. It rejected the plaintiffs' argument that accessing their address books diminished their value, concluding that they failed to tie their allegations that their personal information has value to the alleged injury they suffered. It rejected, however, the App Developers' standing argument with respect to the plaintiff's statutory claim and common law invasion of privacy claim, finding that standing with respect to both was satisfied. The district court also dismissed the plaintiffs' unfair competition law claims for lack of statutory standing, concluding that the plaintiffs failed to show that they "lost money or property" due to the App Developers violations of the statute.

The district court dismissed the public disclosure of private facts claim, ruling that the interception of address book information by third parties does not constitute a disclosure to the public *at large*, and therefore does not constitute a disclosure of private fact. The district court similarly dismissed the Electronic Communications Privacy Act claim and the Texas and California Wiretap Act claims, finding that the allegations did not give rise to an inference that the App Developers "intercepted" any data – rather, the allegations showed only that "different memory components of the same device" used the address book data. The district court also dismissed the Texas Theft Liability Act claim, concluding that there was no allegation that the App Developers deprived the plaintiffs of access to their address books.

The district court denied the App Developers' motion to dismiss the intrusion upon seclusion claim, ruling that the surreptitious retention of the plaintiffs' private contact information was not consensual, was sufficiently offensive, and raised a damages issue regarding the plaintiffs' anxiety, embarrassment, humiliation, and the like.

Facebook and Gowalla. The plaintiffs sought to obtain relief from Facebook because it acquired all of Gowalla's assets. The district court dismissed the Uniform Fraudulent Transfer Act because the plaintiffs' allegations could not establish that there was a "transfer of assets" within the meaning of the statute; Gowalla, for example, retained its intellectual property, which

the plaintiffs could subject to the payment of any litigation debt. The district court dismissed the successor liability claim for the same reason.

In re Hulu Privacy Litigation, 2014 WL 1724344 (N.D. Cal. 2014) (April 28, 2014).

The plaintiffs sued Hulu for violation of the Video Privacy Protection Act for disclosing their video viewing selections and personal identification information to third-party metrics companies and Facebook. Hulu moved for summary judgment, arguing that (1) it disclosed only anonymous user identification information, (2) it did not disclose the information knowingly, and (3) the plaintiffs consented to the social network/Facebook disclosures. The district court mostly agreed with the plaintiffs, permitting much of the case to move to trial. The district court entered judgment in Hulu's favor on its disclosures to the metrics companies, concluding that these disclosures did not tie the identified person to the plaintiff's video habits. But it refused to enter judgment on the disclosures to Facebook because Facebook had enough information with the disclosures to tie identifying information to what a plaintiff was watching. The court rejected Hulu's remaining contentions, ruling that there was enough evidence to suggest that Hulu knew the information it was disclosing had identifying capability, and that there was insufficient evidence to suggest that Hulu had a policy in place in which it sought a consumer's consent to disclose the information.

Robins v. Spokeo, Inc., 742 F.3d 409 (9th Cir. 2014) (Feb. 4, 2014).

Spokeo operates a website that provides users with information about other individuals. The plaintiff sued Spokeo for violation of the Fair Credit Reporting Act for providing false information about him on Spokeo's website. Spokeo moved to dismiss this claim for lack of standing. The district court agreed. The Ninth Circuit reversed, holding that (1) a plaintiff can suffer a violation of a statutory right without suffering actual damages, (2) the plaintiff in this particular case suffered a concrete and particularized injury in his handling of his credit information, and (3) the statutory monetary damages sought could redress the FCRA violation. The cert petition for this case is currently pending before the Supreme Court. The Court called for the views of the Solicitor General on October 6, 2014.

Data Security Litigation

In re Target Corp. Customer Data Security Breach Litigation, -- F. Supp. 3d –, 2014 WL 67753142014 WL 6775314 (D. Minn. 2014) (Dec. 2, 2014) (financial institution cases); *In re Target Corp. Customer Data Security Breach Litigation*, -- F. Supp. 3d –, 2014 WL 7192478 (D. Minn. 2014) (Dec. 18, 2014) (customer cases).

A group of financial institutions and consumers filed suit against Target in the wake of Target's 2013 data breach involving the theft of card information for approximately 110 million customers.

The financial institutions alleged four claims: (1) negligence in failing to provide sufficient data security; (2) violation of Minnesota's Plastic Security Card Act; (3) negligence *per se* (for

violation of the Minnesota Plastic Security Card Act); and (4) negligent misrepresentation due to Target's undue delay in notifying the institutions of the breach. Target moved to dismiss, mostly unsuccessfully. Although the court dismissed the negligent misrepresentation claim because the institutions failed to plead sufficiently that they relied on Target's omission, the court sustained the remaining claims. It ruled that the financial institutions' allegations that Target disabled certain security features in its systems and failed to heed FireEye warnings indicating an intrusion were sufficient to sustain a negligence claim. The Court found that for purposes of the motion to dismiss Target was in a "special relationship" with the plaintiff financial institutions, and thus owed such institutions a duty to protect them from the harmful acts of a third party (namely, the cyber criminals). Target could not claim that owing a duty of care to plaintiffs was an undue burden, the court reasoned, because the company had already assumed such duties in its agreements with Visa and MasterCard. The Court also found that even in the absence of a special relationship, the financial institutions had sufficiently pleaded that their injuries were caused by the direct failures of Target (i.e., inadequate data security and failure to heed warnings of breach, etc.), and thus Target could be held liable.

The consumers alleged several claims: (1) violation of state consumer protection laws; (2) violation of state data breach laws; (3) negligence in failing to safeguard consumer data; (4) breach of contract; (5) bailment; and (6) unjust enrichment. Target moved to dismiss. The court mostly sided with the plaintiffs. With respect to standing, the court concluded that the issue was better suited for resolution at summary judgment or perhaps class certification. With respect to failure to state a claim, the court dismissed several claims on various grounds: for states that follow the economic loss rule, tort claims were dismissed; for states that do not permit mass actions for consumer protection or data breach violations, those claims were dismissed; the bailment claim was dismissed because there was no allegation suggesting an agreement between Target and the plaintiffs to hold the plaintiffs' information; the breach of contract claim was dismissed (without prejudice) to permit the plaintiffs to replead how any contracts were breached and what specific provisions. The rest of the claims survived, including an unjust enrichment claim premised on the allegation that the customers would not have shopped at Target had they known of the breach.

Remijas v. The Neiman Marcus Group LLC, 2014 WL 4627893 (N.D. Ill. 2014) (Sept. 16, 2014).

Several customer-plaintiffs sued Neiman Marcus for negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of state data breach laws, alleging that Neiman Marcus failed to adequately protect against a major data breach and failed to provide timely notice of the breach once it happened. The customer-plaintiffs alleged that Neiman Marcus' conduct left them at an increased risk of identity theft, decreased the value of their private information, and cost them time and money in resolving fraudulent charges and implementing further protections against the risk of future identity theft. Neiman Marcus moved to dismiss the case for lack of standing. The district court agreed, concluding that: (1) the increased risk of future identity theft was not an "injury" under Article III because it did not constitute a "certainly impending" risk; (2) derivatively, the costs incurred from purchasing identity theft protections for future identity theft could not be an Article III injury; (3) the unauthorized credit card charges for which none of the plaintiffs were financially

responsible did not qualify as "concrete" injuries; (4) the expensive quality of Neiman Marcus goods did not create a deficiency-in-value theory of standing (*i.e.*, that the plaintiffs paid a premium in part for added protection is not an Article III injury); and (5) the plaintiffs' loss of control and value of their private information was not sufficiently concrete to constitute an Article III injury. The claims were dismissed.

In re Adobe Systems, Inc. Privacy Litigation, -- F. Supp. 2d – (N.D. Cal. 2014) (Sept. 4, 2014).

The plaintiffs' information was decrypted, stolen, and placed on the internet during and after Adobe's 2013 data breach. They sued Adobe for violation of the California Customer Records Act, the California unfair competition law, breach of contract, and they sought declaratory relief, alleging that Adobe had insufficient protective controls and did not provide reasonable notification of the breach. Their damages were premised on their increased risk of future harm, the cost to mitigate the risk of future harm, and the loss of the value of their Adobe products. Adobe moved to dismiss the claims for lack of standing and failure to state a claim. The court mostly agreed with the plaintiffs. With respect to standing, the court agreed that three types of injury alleged satisfied Article III standing and statutory standing requirements. With respect to failure to state a claim, the court ruled that (most of) the plaintiffs sufficiently plead facts establishing that they relied to their detriment on Adobe's representations regarding its data security measures, the core allegation underlying all of the statutory claims. The court dismissed (with leave to amend) the plaintiffs' claim premise on Adobe's delay in notification, concluding that the plaintiffs had not alleged an injury specifically arising out of the delay.

In re Sony Gaming Networks and Customer Data Security Breach Litigation, 996 F. Supp. 2d 942 (S.D. Cal. 2014) (Jan. 21, 2014).

In 2011, Sony's video game online network was hacked. The plaintiffs in this class action alleged that the hackers stole the personal information of millions of Sony customers, and that Sony unduly delayed in notifying its customers of the intrusion and theft. They asserted several causes of action: negligence, negligent misrepresentation, breach of (implied and express) warranty, unjust enrichment, violation of stat consumer protection statutes, violation of the California Database Breach Act, violation of the Fair Credit Reporting Act, and breach of the covenant of good faith and fair dealing. Sony moved to dismiss the claims for lack of standing and failure to state a claim. The opinion is almost 80 pages, but the abbreviated version is as follows.

With respect to standing, the plaintiffs prevailed. The district court noted that the plaintiffs only needed to plausibly allege a "credible threat of impending harm" due to the disclosure of their personal information following the data breach. The court held that standard was met.

With respect to failing to state a claim, the plaintiffs won a narrow but important victory. Plaintiffs' contract and tort claims were mostly dismissed. The contract claims were subject to warranty disclaimers and contractual liability exclusions that the court held were enforceable; the tort claims were barred primarily because of the economic loss doctrine. The federal Fair Credit Reporting Act claim was dismissed because Sony was not a qualifying consumer reporting

agency. The misrepresentation and certain state consumer protection law claims were also dismissed, except for the claims premised on Sony's (1) affirmative misrepresentation that it had implemented "reasonable security" and "industry-standard encryption," and (2) untimely delay in disclosing the intrusion. Of the surviving state consumer protection law claims, the court dismissed plaintiffs' claims for damages, leaving them only the possibility of equitable relief.

Government Access Litigation

Jewel v. National Security Agency, 2015 WL 545925 (N.D. Cal. 2015) (Feb. 10, 2015).

The plaintiffs sued the NSA for violations of the Fourth Amendment, arguing that the Government collects their internet communications for national security-related intelligence gathering purposes. The NSA moved for judgment, contending that the plaintiffs did not have standing and that the state secrets privilege barred disclosure of information relevant to the suit. The district court agreed with the NSA. With respect to standing, the court concluded that the plaintiffs did not supply sufficient information describing what or how their data is processed by the NSA; moreover, the court's review of classified information contradicted the plaintiffs' accounts. Assuming standing could be met, the court concluded that continued litigation would result in disclosure of classified information protected by the state secrets privilege – information that would have a substantial impact on national security. All of the evidence was, therefore, excluded, and judgment was entered in favor of the NSA.

United States v. Davis, 754 F.3d 1205 (11th Cir. 2014) (June 11, 2014). **Vacated by order granting rehearing en banc (Sept. 4, 2014).**

Davis was convicted of several counts of robbery, conspiracy, and possession of a firearm during a crime of violence. He challenged the admission of location evidence based on stored cell site information obtained by the Government without a warrant. The district court denied the motion. The Eleventh Circuit held that cell site location information *is* within the subscriber's reasonable expectation of privacy, and thus that gaining that such information without a warrant and/or without probable cause is a violation of the Fourth Amendment , but it ultimately affirmed the district court, concluding that the good faith exception saved the Government's conduct in this case. Its ruling created a conflict with the Fifth and Third Circuits. The Eleventh Circuit is rehearing this case en banc, however, vacating the panel opinion.

Riley v. California, United States v. Wurie, 134 S. Ct. 2473 (2014) (June 25, 2014).

The Court held that the police may not conduct a search of digital information on a cell phone seized from an arrested individual without a search warrant. Put differently, the Court concluded that the search incident to arrest exception to the warrant requirement did not encompass a search of a person's cell phone. The Chief Justice's opinion for the Court noted that cell phones may reveal "detailed information about all aspects of a person's life" through browsing history, geolocation data, apps, etc. Justice Alito wrote separately to note that his opinion might be changed if Congress or state legislatures acted to regulate cell phone searches of arrestees.

In re Warrant to Search a Certain E-Mail Account, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (April 25, 2014).

Microsoft moved to quash a search warrant commanding it to produce the contents of one of its customer's emails stored on a server in Dublin, Ireland. Microsoft contended that U.S. courts are without authority to issue warrants for extraterritorial search and seizure. The court denied the motion, concluding that the Stored Communications Act requires an entity receiving a subpoena to comply and produce relevant information regardless of where that information is stored. Microsoft is appealing that decision. The Second Circuit will likely hear argument in the summer of 2015.

Numerous telecom and tech companies have filed amicus briefs in support of Microsoft. The arguments center on the availability of the MLAT process, respect for foreign laws, comity and balancing tests, and the adverse impact that the ruling could have an the ability of US business to compete for foreign (especially European) digital commerce.