SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks, Insurance Coverage, Data Breach, and Standing Decisions January through April 2017

Vincent J. Vitkowsky

New York Connecticut New Jersey

SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks, Insurance Coverage, Data Breach, and Standing Decisions January through April 2017

Coverage Decisions

Media Liability Coverage under Cyber Policy

New York Appellate Division Applies Retroactive Date Exclusion and Unfair Practices Exclusion To Deny Coverage under a Comprehensive Cyber Policy

LifeLock, Inc. v. Certain Underwriters at Lloyd's, 2017 WL 161045 (N.Y. App. Div. Jan. 17, 2017). The First Department affirmed the dismissal of claims seeking media liability coverage under an Information Security, Privacy Liability, First Party Data Protection and Network Business Interruption Insurance Policy.

LifeLock is an identity theft protection company. It was sued in several class actions asserting that, through statements on its website, it had engaged in fraudulent and deceptive practices to induce customers to enter into contracts that did not provide the protections it promised.

The Retroactive Date Exclusion precluded coverage for "related or continuing acts ... where the first such act … was committed or occurred prior to the Retroactive Date." The statements first appeared on LifeLock's website in 2005 and remained after the Retroactive Date of January 8, 2008. Underwriters argued that there was pattern of false and misleading advertising beginning in 2005, so the Exclusion applied. The court agreed. In addition, Underwriters argued that the claims fell within the Exclusion for Unfair Trade Practices. Again, the court agreed.

Data Breach Coverage under Management and D&O Policy

Texas Federal District Court Dismisses a Claim for Coverage of Attorneys' Fees Incurred to Recover PCI Fees and Fines Withheld by a Card Processor

Spec's Family Partners Ltd. v. Hanover Ins. Co., Case. No. 4:16-cv-00438 (U.S.D.C., S.D. Tex. March 15, 2017). A federal court in Texas dismissed a retailer's claim for coverage of attorneys' fees incurred in an action to recover PCI fees and fines withheld by a card processor. The decision was based on the absence of coverage because of the contractual liability exclusion.

The case arose under a Private Company Management Liability Policy with a Directors, Officers and Corporate Liability Coverage Part issued by Hanover Insurance Company to Spec's, a chain of liquor stores in Texas. Spec's suffered two data breaches of its credit card payment system. Its transactions were processed pursuant to a Merchant Agreement with First Data Merchant Services, LLC.

Visa and MasterCard issued $9.5 million in case management fees and assessed fines (collectively, "fines"). First Data sent two letters to Spec's for claims arising from the data breaches. To satisfy its demands, First Data withheld $4.2 million from daily payment card settlements for Spec's and used the money to establish a reserve account. Spec's sued First Data to seek recovery of the withheld amounts. It also sued Hanover, which had entered into a Defense Funding Agreement ("DFA"), arguing that Hanover should pay for its lawyers in the action against First Data.

The court granted Hanover's motion to dismiss on the pleadings, resolving the case by holding that there was no duty to defend of any kind, because coverage was precluded by the exclusion for liability under a contract.

The policy gave Hanover the right and duty to defend a "Claim," which was defined to include a written demand for monetary damages for a Wrongful Act. The court found that the fines were levied against the card processor, First Data, and did not represent a separate demand against Spec's, so were not a Claim under the policy. Rather, the Claim was made in the demand letters for indemnification under the Merchant Agreement.

In applying the contractual exclusion, the court reviewed the DFA to determine whether it modified the exclusion, and concluded it did not, because in the DFA, Hanover reserved its rights to challenge its duty of defense or to withdraw its defense. The court went on to reject the contention that the fines and the funding of a reserve account did not arise out of the contract with First Data, so were covered because the exclusion did not apply if the liability would have attached in the absence of the contract. The court declined "to find a speculative factual scenario or legal theory in which MasterCard or Visa make a claim directly against [the insured]." It found the only Claim was the one for indemnification in the demand letters.

The court also rejected the insured's argument that the hack constituted superseding criminal conduct, which was an independent, "but for" cause of the claim making the contractual exclusion inapplicable. The court held that the only reason for the liability of Spec's to First Data was the Merchant Agreement.

Coverage under Crime Policies

Georgia Federal District Court Holds There is No Computer Fraud Coverage for a Loss Enabled by a Coding Error

InComm Holdings, Inc. v. Great American Ins. Co., Case No. 1:15-cv-2671 (U.S.D.C., D. Ga. March 16, 2017). The court found no coverage under a Computer Fraud policy for claims arising from a scheme involving a Prepaid Debit Card Plan.

The insured, InComm, was a debit card processor providing a service enabling customers to load funds onto prepaid debit cards issued by banks. Debit card holders purchased "chits" from retailers, such as CVS or Walgreens, for the amount of the chit plus a service fee. InComm's computers allowed debit card holders to request transactions on their account, including redeeming the chits to load funds onto their cards, using telephone voice commands or touch-tone codes. With the redemption, InComm would transfer funds to the banks. However, there was a coding error in InComm's computer system. If cardholders used more than one telephone simultaneously to redeem the same chit, they would be credited with multiples of the amount of the chit. In a well-organized scheme, a criminal ring redeemed 1,933 chits an average of 13 times, for a total of

25,553 unauthorized redemptions, with a total value of $11,477,287. The scheme spread over 28 states, and many of the purported individual "holders" of the relevant debit cards were victim of identity theft.

Great American's policy provides coverage for Computer Fraud, insuring against "loss of …money … resulting *directly* from the *use* of any *computer* to fraudulently cause a transfer …." (Emphasis added.) Applying Georgia law, the court granted Great American's motion for summary judgment. First, it found that the wrongdoers did not use a computer to make the redemptions. They used a telephone. It said "[A] person thus 'uses' a computer where he takes, holds or employs it to accomplish something. That a computer was somehow involved in a loss does not establish that the wrongdoer 'used' a computer to cause a loss." It went on to hold that even if a computer *had* been used, the "loss" did not result "directly" from that use. Nor did it result "directly" from the initial fraudulent redemptions, because they did not automatically cause the transfer of funds. Instead, the "loss" did not occur until the funds held by the banks were used to pay sellers for purchases made by the wrongdoers. Rather, the loss occurred because InComm itself chose to make transfers to the banks, and it was that decision that resulted "directly" in the loss.

Ninth Circuit Finds No Coverage under a Crime Policy for Social Engineering Business email Fraud

Taylor & Lieberman v. Federal Ins. Co., 2017 WL 929211 (9th Cir. Mar. 9, 2017) (unpublished). The Ninth Circuit held that an accounting and business management firm that fell victim to a social engineering fraud did not have coverage under any of the insuring agreements of a Crime policy.

The insured received two emails from a client's hijacked email account, directing funds transfers to accounts in Malaysia and Singapore. It complied. The insured then received a third email purportedly from the client, but from another email address, directing a third transfer. The insured called the client and learned that all three emails were fraudulent.

The Forgery grant applied to "forgery or alteration of a financial instrument." The insured argued quaintly that under the "Last Antecedent Rule," the word" alteration" only applied to "financial instruments", but a forgery of any kind would be covered. The court rejected that construction, and found that the fraudulent emails were not financial instruments.

The Computer Fraud grant applied to unauthorized entry into the insured's computer system, and the introduction of instructions that propagated themselves through that system. The court applied the plain meaning rule to hold that (1) sending an email does not constitute unauthorized entry into a system, because the policy was designed to cover matters like the introduction of malicious code, and (2) the emails did not propagate themselves through the computer system.

Finally, the Funds Transfer Fraud grant encompassed "fraudulent … electronic … instructions issued to a financial institution directing such institution to transfer … money … from any account maintained by the [insured] at such institution, without the [insured's] knowledge or consent." The court found that the coverage was inapplicable because the insured knew about the transfers (it had requested them). The court also held that the receipt of emails purportedly from the insured's client to the insured does not trigger coverage because the insured was not a financial institution.

The lower court had found for Federal on the grounds that the insured's loss was not "direct." The Ninth Circuit did not address this ground, but affirmed summary judgment on other grounds. Thus it left the lower court's holding on the additional point undisturbed.

Data Breach Decisions

Decisions on Causes of Action Relating to Data Breaches

Pennsylvania Intermediate Appellate Court Finds No Duty to Protect Employee Information from a Data Breach

Dittman v. UPMC, 2017 PA Super 8, 2017 WL 117652 (Pa. Super. Ct. Jan. 12, 2017). The Pennsylvania Superior Court affirmed the dismissal of claims against an employer resulting from a breach of electronically-stored personal and private information.

The University of Pittsburgh Medical Center (UPMC) suffered a data breach exposing information about its 62,000 present and former employees. At least 788 of those employees were subsequently victims of

tax fraud. The employees asserted that UPMC breached a legal duty to protect their information, specifically by failing to properly encrypt data, establish adequate firewalls, and implement adequate authentication procedures. The court held that no such legal duty existed.

The court applied the Pennsylvania test to determine whether a duty exists, which requires consideration of five factors. The first factor is the relationship between the parties. Although the employer-employee relationship traditionally include duties by employers, and thus this factor weighed in favor of imposing a duty, the court did not view this as controlling. The test goes on weigh two further factors, which are the "social utility of the actor's conduct" and "the nature of the risk imposed and foreseeability of harm incurred." The court concluded that while a data breach is generally foreseeable, that possibility does not outweigh the social utility and efficiency of storing information electronically. This balancing weighed against imposing a duty on UPMC. (The court strongly implied that if there had been allegations of specific threats and problems with UPMC's computer system before the breach occurred, the balancing might have come out differently.) The fourth factor is the consequences of imposing a duty. The court stated there was no need to further incentivize companies to protect confidential information, and recognized that companies would be required to incur potentially significant costs to increase security measures even though it is not possible to prevent data breaches altogether. It concluded that this factor weighs in favor of not imposing a duty. The final factor is the public interest in imposing a duty. Here the court accepted the trial court's view that because the legislature has specifically addressed data breaches, and has required only that notice be provided, the public interest would not be served by "judicial action that disrupts that [legislative] deliberation process." It also stated that creating a duty would "greatly expend judicial resources." Thus it found this factor weighed against creating a duty.

In addition, the court held that the economic loss doctrine prevented recovery in tort for solely economic damages unaccompanied by physical injury or property damage. Finally, the court held that there was no implied contract to protect the information, because there were no objective manifestations of intent to enter into such a contract, nor was any consideration paid.

Pennsylvania Federal District Court Dismisses Contract Claims against Employer in Data Breach

Enslin v. The Coca-Cola Co., No. 2:14-cv-06476 (U.S.D.C., E.D. Pa. March 31, 2017). A federal court in Pennsylvania rejected claims that Coca-Cola had contractual duties to protect a former employee's personal data.

An IT employee of Coca-Cola took home laptop computers that were no longer in use, keeping some and giving others away. Some of those were previously used by HR personnel, and thus had personal information of 74,000 current and former employees. A few months after being notified of the breach, some of the plaintiff's accounts with online retailers were compromised. The plaintiff asserted that the company's employment application, its Code of Business Conduct, and two detailed information technology policies gave rise to a contractual duty to protect his information. Both sides moved for summary judgment.

The plaintiff was a member of the Teamsters Union, so as a preliminary matter, the court had to conclude that the collective bargaining agreements with the Teamsters did not pre-empt state law claims or subject plaintiff to a grievance procedure which he did not follow. It reached this conclusion because neither collective bargaining agreement contained any terms relating to the safeguarding of personal information. The court held that portions of the Code of Conduct did create enforceable obligations, but none of the provisions in it or the policies or the employment agreement constituted a promise on the part of the company to safeguard personal information. Nor would the court imply such a term. It also declined to find an implied contract to safeguard personal information, citing to a Third Circuit case and to ***Dittman v. UPMC*** (see discussion above).

The court also rejected an unjust enrichment claim seeking restitution under the "opportunistic breach" theory, based on its earlier conclusion that there were no relevant contractual duties to breach.

Previously, in 2015, the court had dismissed, on the pleadings, plaintiff's claims for negligence, negligent misrepresentation, fraud, bailment, civil conspiracy, and violation of the Driver's Privacy Protection Act of 1994.

Pennsylvania Federal District Court Allows Financial Institutions to Press Negligence, Negligence Per Se, and State Statutory Claims against Wendy's

First Choice Federal Credit Union v. The Wendy's Company**,** 2017 WL 1190500 (U.S.D.C., W.D. Pa. Mar. 31, 2017). On a motion to dismiss on the pleadings, the court adopted the report and recommendation of a magistrate, allowing claims brought by 26 financial institutions to proceed against Wendy's in connection with the data breach it suffered from hackers in 2015 and 2016.

As an initial matter, the magistrate was asked to make a choice of law ruling because of differences in the application of the economic loss doctrine. Wendy's urged for Ohio law, its home state, but plaintiffs urged that the laws of their various principal places of business should apply. This contest related to whether the loss of computer data can be considered property under the economic loss doctrine. The magistrate found that "it is not implausible that computer data could be considered property in this context," and thus it was plausible that the economic loss doctrine might not apply, so the magistrate declined to undertake a choice of law analysis at the early stage, prior to discovery.

Plaintiffs alleged specific acts and omissions in safeguarding payment card data, which the magistrate concluded were sufficient to advance a plausible claim for negligence. Plaintiffs also alleged that the failure to use reasonable measures to protect data and to comply with applicable industry standards violated Section 5 of the Federal Trade Commission Act and similar state statutes, and thus constituted negligence per se. Relying on and applying a 2016 ruling to that effect in the Home Depot data breach litigation, the magistrate allowed these claims to proceed. Plaintiffs further alleged that Wendy's violated the Ohio Deceptive Trade Practices Act by misrepresenting its security, and that they were damaged as a direct and proximate result. The magistrate took these allegations as sufficient to plead reliance, and ruled that these claims were plausible enough to proceed.

Finally, the magistrate declined to dismiss claims seeking declaratory and injunctive relief, because the claims assert continuing action by Wendy's,

and found that the financial institutions could rely on the associational standing of their members to seek such relief.

In Premera Data Breach Case, Oregon Federal District Court Allows Various Tort and Contract-Based Claims to Proceed, Dismisses Others

In re Premera Blue Cross Customer Data Security Breach Litigation, 2017 WL 539578 (U.S.D.C., D. Or. Feb. 9, 2017). This is a putative class action alleging various state common law tort, contract, and statutory claims under Washington and Oregon law. Premera is a healthcare benefits servicer and provider which suffered a breach of its network, compromising the Personal Information of 11 million current and former members, affiliated members, and employees. Premera moved to dismiss the pleadings under Fed.R.Civ. P. 9(b).

As to the tort-based claims, plaintiffs alleged that Premera's policy booklets, Privacy Notice, and Code of Conduct contained affirmative misrepresentations under the Washington Consumer Protection Act ("WCPA"). The court observed that Washington law does not require reliance, and proximate cause is an issue of fact. It held that one of the booklets, the "Preferred Select" policy booklet, contained sufficiently specific representations that Premera would "make sure" that information remained secure, and plaintiffs alleged that the statement was false because Premera did not "make sure" the information was protected, but rather knew it had inadequate data security measures. However, even though the "Preferred Bronze" policy booklet stated that Premera "takes care" to ensure that information remains confidential by having a company confidentiality policy and by requiring all employees to sign it, Plaintiffs did not allege that Premera did not have such a policy or did not require its employees to sign it. Thus the court found that the allegations relating to that policy were insufficient to allege affirmative misrepresentation.

Premera's Privacy Notice contained various alleged misrepresentations on data security. These included Premera's committing to maintaining confidentiality, stating it took measures to comply with federal and state privacy laws, limiting authorized access to personal information, securing buildings and systems from unauthorized access, employee training, and protecting the information of former members. The court found that these representations, if false, were sufficient to support a claim of affirmative

misrepresentation, so it allowed claims to stand as to plaintiffs who were provided with the Privacy Notice.

Premera's website contained a Code of Conduct, and Premera argued that certain statements on it were not deceptive because they were mere "puffery" or expressions of corporate optimism. The court found that the statements had the capacity to deceive and thus were sufficient to support a claim for deceptive statements under the WCPA.

The court found the plaintiffs did not allege facts demonstrating the tort of active concealment, so it dismissed those claims. However, it allowed the claims sounding in fraud by omission to stand. It found plaintiffs alleged that Premera should have disclosed that it did not implement industry standard access controls, did not fix known vulnerabilities in its electronic security protocols, failed to protect against reasonable anticipated threats, and otherwise did not comport with its assurances regarding protecting information. Finally, plaintiffs argued that their allegations that Premera's conduct was unfair under the WCPA, were not subject to federal pleading requirements. The court disagreed, holding that those allegations were based upon deceptions, so federal pleading requirements applied, and were met (or not) according to it earlier rulings.

As to the contract-based claims, using the factual analysis it used for the tort claims, the court held that claims were sufficiently pleaded for breach of express contract by policyholders who were sent the Preferred Select policy booklet, but not the Preferred Bronze policy booklet, and for plaintiffs who received the Privacy Notice. The statements in the Code of Conduct, which were found to be sufficiently "deceptive" under the WCPA, were held to not be enforceable promises sufficient to support an express breach of contract claim.

The court found that for contracts governed by Washington law, there was no basis for a claim of breach of an implied contract term that adequate data security measures would be taken. However, for those contracts governed by Oregon law, it *was* appropriate to imply such a term. It rejected Premera's argument that implying a data security term would frustrate the purpose of Congress in not allowing a private right of action under HIPAA.

Plaintiffs also alleged the existence of implied-in-fact contracts for the provision of data security, separate from any express contracts. The court allowed this claim to proceed by policyholder plaintiffs, but dismissed it as to non-policyholder plaintiffs. It reasoned that because the overall contractual relationship necessarily required the provision of sensitive information, it was a plausible inference that plaintiffs understood and intended that Premera would adequately protect that information.

Finally, Premera sought to dismiss the claims on the grounds they are completely preempted under ERISA. Plaintiffs had identified specific provisions in the policy booklets and other documents that they allege were incorporated into their health benefits contract. Section 502(a) of ERISA allows civil enforcement claims to be brought by a participant (1) to recover benefits under the plan, (2) to enforce his rights under the terms of the plan, or (3) to clarify rights as to future benefits under the plan. The court found that data security was not an ERISA "benefit", so the only claims that might constitute ERISA claims were those "to enforce rights under the terms of the plan," because those claims were not limited to "benefits." However, the court found that although there is some relationship between data security and the administration of the ERISA plan, it was insufficient to overcome the presumption against preemption of state law, so plaintiffs' claims were not preempted.

California Federal District Court Allows Implied Contract, Negligence and Statutory Unfair Competition Claims to Proceed

Walters v. Kimpton Hotel & Restaurant Group. LLC, Case. No. 15-cv-05387 (U.S.D.C., N.D. Cal. April 13, 2017). Ruling on a motion to dismiss, the court found that a plaintiff who had been a guest at a hotel chain that suffered a data breach had asserted plausible claims in implied contract, negligence, and violation of the California Unfair Competition Law.

Hackers allegedly accessed Kimpton Hotels' computer systems across the U.S. The court found that because plaintiff was a guest during the at-risk window, it was plausible to infer that his payment card information was stolen.

The court allowed a claim to proceed that alleged the existence of an implied contract arising from Kimpton's privacy policy, which states that Kimpton is "committed" to safeguarding customer privacy and personal

information. It found that plaintiff had suffered actual damages, including having to secure and maintain credit monitoring services and out-of-pocket expenses, and the value of time reasonably incurred to remedy or mitigate the breach. Next, the court allowed the negligence claim to proceed, merely noting that plaintiff had suffered actual damages. The court also ruled it lacked sufficient information to dismiss based on the economic loss doctrine at this stage. Third, it allowed claims for unfair and unlawful business practices under the California Unfair Competition Law to proceed, again because the plaintiff alleged economic injury. However, it dismissed a claim under the statute based on fraud because plaintiff had failed to plead reliance on Kimpton's alleged misrepresentations.

The court also found that plaintiff had standing, because he plausibly alleged "that his data had already been stolen and that it was taken in a manner that suggests it will be misused." (See the additional cases on standing below.)

Decisions on Article III Standing Relating To Data Breaches

Third Circuit Holds that Alleged Violations of the Fair Credit Reporting Act Concerning Disclosure of Personal Information through a Data Breach Are Sufficient to Establish Article III Standing

In re Horizon Healthcare Services, Inc. Data Breach Litigation, 846 F. 3d 625, 2017 WL 242554 (3rd Cir. Jan. 20, 2017). The Third Circuit held that with the passage of the Fair Credit Reporting Act (FCRA), Congress established that the unauthorized dissemination of personal information by a credit reporting agency in and of itself causes an injury sufficient to establish Article III standing.

Two laptops containing unencrypted personal information of more than 839,000 Horizon members were stolen. Plaintiffs in a putative class action alleged willful and negligent violations of the FCRA. There were no allegations that identities were stolen as a result of the breach. (Although one plaintiff alleged he was the victim of a fraudulent tax return and a denial of credit, the court did not reach his argument.)

The court found there was no doubt that plaintiffs had alleged a particularized injury, because they alleged the disclosure of their own

private information. Thus, the court only addressed the concreteness requirement of the injury-in-fact element of standing. It recognized established authority that the violation of a statute creating legal rights can cause an injury in fact sufficient for standing. The court held that with the passage of the FCRA, Congress established that the mere unauthorized dissemination by a credit reporting company causes an injury, even though the information is truthful and not harmful to anyone's reputation. It stated that Congress provided for damages for willful violations, which shows that Congress believed that FCRA violations cause concrete harm. That is, Congress "elevated the unauthorized disclosure of [credit] information into a tort."

The court rejected arguments that ***Spokeo, Inc. v. Robins,*** 136 S. Ct.1540 (2016) compelled a different outcome. It concluded that ***Spokeo*** did not create a requirement that plaintiffs show that a statutory violation has caused a "material risk of harm" to establish standing.

There are separate issues of whether Horizon is a "consumer reporting agency" subject to the FCRA, and whether the FCRA applies when data is stolen rather than voluntarily furnished. Those are subject to another motion on which the district court had not ruled, so they were not yet before the appellate court.

Fourth Circuit Holds that Increased Risk of Future Identity Theft Does Not Establish Article III Standing

Beck v. McDonald, 848 F. 3d (4th Cir. Feb 6, 2017). Continuing a split among the federal circuit courts, the Fourth Circuit affirmed a district court's holding that allegations of an increased risk of identity theft are insufficient to establish the non-speculative, imminent injury-in-fact required for Article III standing.

The court consolidated cases involving two breaches at a Veteran Affairs Medical Center. The first involved the likely theft of an unencrypted laptop with personal information of over 7,400 patients. The second involved the loss or theft of four boxes of pathology reports containing identifying information and medical diagnoses of 2,000 patients. The plaintiffs alleged violations of the Privacy Act of 1974 and the Administrative Procedure Act.

The court focused on the injury-in-fact element, and found that "threatened injury'" was not "certainly impending" as required by ***Clapper v. Amnesty International USA***, 133 S. Ct. 1138 (2013). It also rejected plaintiffs' claims that "emotional upset" and "fear [of] identity theft and financial fraud" are adverse effects sufficient to confer standing. The court acknowledged a difference in federal circuits, noting that the Sixth, Seventh, and Ninth Circuits have recognized, at the pleading stage, that the threatened injury of identity theft can establish an injury-in-fact, but the First and Third Circuits have not. It stated, however, that in the cases finding standing, there were allegations that pushed the threatened injury of future identity theft beyond the speculative to the sufficiently imminent. For example, those cases involved hackers who intentionally targeted personal information, and in one there was an allegation of specific misuse of the information. No such allegations were made in the present case, rendering the risk of future identity theft too speculative. The mere theft of a laptop and boxes did not indicate that the private information had been targeted or accessed.

In addressing a potential second basis for standing, the court declined to find a "substantial risk" that harm will occur, leading a party to reasonably incur mitigation or avoidance costs. It also declined to follow other circuits which inferred a substantial risk of future identity theft from an organization's offer to provide free credit monitoring services. And it held that any mitigation expenses incurred by the plaintiffs were "self-imposed harms [that] cannot confer standing."

Plaintiffs also sought injunctive relief under the Administrative Procedures Act. The court declined to grant that relief because the complaints had not established that there was a sufficient likelihood plaintiffs would be subject to future breaches.

Decisions on Article III Standing in Other Contexts

Eleventh Circuit Holds that Mobile App User Has Article III Standing, but No Status as a Subscriber under Video Privacy Protection Act

Perry v. Cable News Network, Inc., 2017 WL 1505064 (11th Cir. April 27, 2017). The Eleventh Circuit held that the user of a mobile app whose activities were shared without his consent had Article III standing, but yet

had no cause of action for statutory relief under the Video Privacy Protection Act (VPPA).

Plaintiff downloaded the CNN App to his iPhone. Among other things, the App allows a user to view videos. Plaintiff alleges that without a user's knowledge or consent, CNN tracks the views, collects a record, and then forwards that information, together with the user's MAC address (which identifies the specific mobile device) to a data analytics company called Bango. Bango receives other information from an extensive range of networks and devices. As described by the court, "Bango is able to compile personal information, including the user's name, location, phone number, email address, and payment information, and it can attribute this information to a single user across different devices and platforms." Plaintiff alleged a violation of the VPPA, which prohibits a video provider from the knowing disclosure of personally identifiable information of its renters, purchasers, or subscribers.

The court affirmed a decision granting a motion to dismiss on the pleadings, but first found that plaintiff had standing. The court found that the structure and purpose of the VPPA demonstrates that it provided a cause of action for "any person aggrieved." The court said the VPPA protected against a type of invasion of privacy, and such an invasion has long been recognized as a tort by the great majority of jurisdictions. Thus, the court concluded that such a wrongful disclosure by a video provider satisfies the concreteness requirement of Article III standing.

However, the court found that plaintiff lacked the necessary status as a subscriber. The court applied its earlier decision in ***Ellis v. Cartoon Network, Inc.,*** 803 F.3d 1251 (11th Cir. 2015), which held that downloading and using a free app does not make the user a subscriber under the VPPA. In refusing to allow an amended complaint, the court rejected plaintiff's argument that because CNN was part of his cable television package, plaintiff was a subscriber of CNN. It ruled that in the absence of an "ongoing commitment or relationship" with CNN, plaintiff is not a subscriber. Given this disposition, the court was not required to rule on whether a MAC address and video history were "personally identifiable information" under the VPPA

Seventh Circuit Holds that Retention of Personal Information in Violation of the Cable Communications Policy Act Does Not in Itself Establish Article III Standing

Gubala v. Time Warner Cable Inc., 846 F. 3d 909 (7th Cir. Jan. 20, 2017). The Seventh Circuit affirmed a district court's ruling that a cable company's failure to destroy personally identifiable information of former subscribers, without more, is insufficient to establish Article III standing.

Plaintiff was a former subscriber to Time Warner's cable services, who provided personally identifiable information to the company. Eight years after cancelling his service, he inquired and learned that his information was still in the company's possession. He sought injunctive relief for alleged violation of the Cable Communications Policy Act, which provides for the destruction of personally identifiable information when it is no longer necessary for the purpose collected, and there are no pending requests or court orders for access to the information.

Plaintiff did not allege that the information had been misused, sold or given away by the company, nor even allege a *fear* that it might be. He asserted only that the retention of the information violated a privacy right or entailed a financial loss. The court acknowledged that there was some risk of harm, and the statute gives a cause of action to any person aggrieved by a violation of the destruction provision. But the plaintiff provided neither evidence nor even allegations that in fact he had been so aggrieved -- only that he *felt* aggrieved. Thus he had not alleged any risk substantial enough to meet the "concreteness" test of ***Spokeo, Inc. v. Robins***, 136 S. Ct. 1540 2016).

May 2, 2017

Vince Vitkowsky is a partner in Seiger Gfeller Laurie LLP, resident in New York. He represents insurers and reinsurers in coverage matters across many lines of business, including cyber, CGL, and professional liability. He also defends insureds in complex claims. Vince can be reached at vvitkowsky@sgllawgroup.com. Information on Seiger Gfeller Laurie LLP can be found at www.sgllawgroup.com.

Copyright 2017 by Vincent J. Vitkowsky. All rights reserved.