

# 2020-21 Data Privacy and Security Litigation Update



**Sedona Working Group 11 - 2021 Mid-Year Meeting**  
**Data Privacy and Security Litigation Update**  
**Case Summaries**

**Phil Yannella, ed.<sup>1</sup>**

**ACLU v. Clearview, Cook County, Ill. No. 20 CH 4353 (Ill. Cir. Ct. Aug. 27, 2021) (First Amendment/biometrics).**

In a BIPA case against Clearview AI, a software company that provides a facial recognition app based on a screen-scraped database of 3 billion images, the Court denied Defendant's Motion to Dismiss. The court rejected Clearview's defenses of First Amendment protection as well as lack of personal jurisdiction, inapplicability of BIPA to photographs and facial prints derived from photographs, and preclusion due to the dormant commerce clause. In response to defendant's argument that consent under BIPA was not required because the collected photos were "public," it noted "The fact that something has been made public does not mean anyone can do with it as they please." On the First Amendment issue, the court rejected arguments that BIPA's application was content-based and viewpoint discriminatory and passed intermediate scrutiny. Finally, the court rejected Defendant's argument that application of BIPA would reduce the app's effectiveness because it was impossible to distinguish which photographs were Illinois residents, holding that the inability to find a solution to a technological problem it created did not immunize the company from BIPA liability.

**AMG Capital Management v. FTC, U.S. Supreme Court, 141 S. Ct. 1341 (2021)(scope of FTC's restitution authority)**

Appeal from the Ninth Circuit on the question of whether the FTC can seek equitable monetary relief such as restitution and disgorgement under its FTCA §13(b) authority (15 U. S. C. §53(b)), which authorizes the FTC to seek a "permanent injunction." The Supreme Court unanimously held that the FTC does not have statutory authority to pursue such relief directly from the Courts (as opposed to after a respondent has violated a previously entered Consent Order). Petitioner was a payday lender that engaged in deceptive acts and practices in the process of issuing over 5 million payday loans, in the process collecting over \$1.3 billion through deceptive charges. The District Court and Ninth Circuit rejected Petitioner's argument that the FTC lacked statutory authority to seek equitable monetary relief. The Supreme Court held that the FTCA's §13(b) permanent injunction provision did not provide equitable monetary relief through its language taken in the context of the section as a whole, which focused on prospective, not retrospective, relief.

---

<sup>1</sup> Special thanks to WG11 members Ken Withers, Jami Vibbert, and Ryan Kriger for their recommendations and submissions to this case law update.

**Attorney General of the Commonwealth of Massachusetts v. Facebook, 487 Mass. 109 (Mar. 24, 2021)(attorney-client privilege in data breach context).** The Attorney General of Massachusetts issued Civil Investigative Demands to Facebook in the wake of the Cambridge Analytica incident. Specifically, the Attorney General sought information generated by Facebook’s App Developer Investigation (“ADI”) launched in March of 2018 in response to the revelation that Cambridge Analytica had used data obtained through a Facebook app developer to influence the 2016 presidential election in the United States. Facebook refused, on work product and attorney-client privilege grounds, to produce “information generated in the course of its ADI about the specific apps, groups of apps, and app developers that Facebook claims to have flagged as potentially problematic or, at the very least, has identified as worthy of additional examination.” In an enforcement action, the trial court overruled Facebook’s objections, holding that the ADI was not undertaken in anticipation of litigation, but was instead performed for business purposes. *Attorney General v. Facebook*, 1984-CV-02597-BLS1, 2020 WL 742136 (Mass. Super. Ct. Jan 17, 2020). On appeal, the Massachusetts Supreme Judicial Court (SJC) reversed and remanded for further consideration. The unanimous court reasoned that “the ADI is meaningfully distinct from Facebook’s ongoing enforcement program. It is staffed by outside counsel and outside forensic consultants, and it has its own distinct methodology. It is focused on past violations, not ongoing operations, and it serves a very different purpose: defending Facebook against the vast litigation it is facing, rather than just improving its ongoing operations.” The SJC also ruled, however, that despite the finding that the ADI constitutes work product, the Attorney General had shown a “substantial need” for the factual information contained in the report and that there was no other source from which the withheld information could be obtained without “undue hardship.” The SJC could not conclude that *none* of the requested information fell into the protected category of opinion work product. Accordingly, the SJC remanded the matter to the trial court to determine what information constituted fact work product, which would be subject to discovery, as opposed to opinion work product, which would remain protected.

**Brooks v. Thomson Reuters Corp., 21-cv-01418-EMC, 2021 U.S. Dist. Lexis 154093 (N.D. Cal Aug. 16, 2021) (California UCL).** In a case arising out of the collection and sale of detailed personal information, Defendant filed a motion to dismiss plaintiffs’ claims under the California common law of commercial misappropriation and California’s Unfair Competition Law (UCL). Despite finding that the collection and sale of the plaintiffs’ personal information constituted sufficient use to satisfy the misappropriation test, the court held that the plaintiffs’ misappropriation claim must fail because the defendant’s use was not “for promotional purposes” of another product or service. The court similarly dismissed the plaintiffs’ claims that the defendant’s conduct was “unlawful” under the UCL, as these claims relied on the common law misappropriation claims. However, the court upheld the plaintiffs’ claims that the defendant’s conduct was “unfair” under the UCL. The court expressly rejected an argument that the existence of an opt-out mechanism designed to meet the requirements of the California

Consumer Privacy Act (CCPA) necessarily renders dissemination of personal information fair under the UCL. Because the CCPA does not preempt other privacy laws, compliance with the CCPA is not a defense to claims that the sale of personal information is an unfair business practice. Finally, the court found that the collection and sale of the Plaintiffs' personal information could be found unfair under either the balancing test or the tethering test required by the UCL because the extensive collection and sale of personal information constitutes a "tremendous" "all-encompassing invasion" of privacy and California's constitution and privacy legislation clearly demonstrate "California's public policy of protecting consumer data."

**Cothron v. White Castle, 477 F. Supp. 3d 723 (N.D Ill. 2020)(BIPA claim accrual).**

Plaintiff Latrina Cothron worked at a White Castle in Illinois in 2004 when White Castle began using an optional, consent-based finger-scan system for employees to sign documents and access their paystubs and computers. In 2018, she filed a suit against White Castle for purported violations of BIPA, alleging that White Castle did not obtain valid consent to collect or disclose her fingerprints at the first instance the collection occurred under BIPA because BIPA did not exist in 2007 and that her prior consent to the collection of biometric data did not satisfy BIPA's requirements. In addition, she alleged that White Castle violated BIPA Sections 15(b) and 15(d) by collecting, then "systematically and automatically" disclosing, her biometric information without adhering to BIPA's requirements, seeking statutory damages for "each" violation on behalf of herself and a putative class. The District Court disagreed with defendant that plaintiff's Section 15(b) and 15(d) BIPA claims were time barred because they accrued in 2008, with the first scan of plaintiff after BIPA's enactment and that plaintiff could recover for "each violation." Pending Seventh Circuit decision.

**Curling v. Raffensperger, No. 1:17-CV-2989 (N.D. Ga.) (ECF No. 858; Order dated Aug. 2, 2020)(attorney-client privilege).** Years before the 2020 general election, Georgia citizens' groups filed an action to force the state of Georgia to improve its electronic voting system and the security of its voter registration database. The plaintiffs moved to compel production of a report prepared by Fortalice Securities regarding the security of Georgia's ballot-marking devices ("BMDs"). In an unpublished order, the court found that the report was prepared for purposes of litigation at the direction of the General Counsel for the Georgia Secretary of State, that the report would not have been created in substantially the same form without the litigation, and that it was therefore protected as work product. The plaintiffs did not challenge the court's findings but argued that they had a "substantial need" for the information in the report and no other way of obtaining it. The court refused to compel the state to produce the report but required the state to make one of its BMDs available to the plaintiffs for their own inspection.

**Facebook v. Duguid, 141 S. Ct. 1163 (2021) (TCPA).** In a class action against Facebook for use of an automated text messaging system for account alerts, the Supreme Court clarified the

definition of an “auto-dialer” under the Telephone Consumer Protection Act (TCPA). Among other things, the TCPA restricts the use of automatic telephone dialing systems, defined as a “piece of equipment with the capacity to both store or produce telephone numbers to be called, using a random or sequential number generator, and to dial those numbers.” The question before the court was whether this definition “encompasses equipment that can store and dial telephone numbers, even if the device does not use a random or sequential number generator.” Relying on a basic textual analysis of the Act, a unanimous Supreme Court held that it does not. The Supreme Court found that expanding the definition of auto-dialer “to encompass any equipment that merely stores and dials telephone numbers” would defy established grammatical rules as well as Congress’s intent in passing the law. It further rejected plaintiff’s arguments that the definition of auto-dialer should be read more expansively to keep up with the progress of technology. It found that this argument was better suited for Congress than the Court, which was obligated to follow “the best reading” of the Act. As a result, the Court held that a necessary feature of an auto-dialer under the TCPA was the use of a random or sequential number generator to either store or produce the phone numbers to be called.

**Fernandez v. Kerry, 2020 U.S. Dist. LEXIS 223075 (7<sup>th</sup> Cir., No. 30, 2020) (BIPA preemption under LMRA).**

Employees brought an action against employer, Kerry, Inc., for violations of the Illinois Biometric Information Privacy Act (“BIPA”) based on an alleged failure by the employer to obtain consent before requiring their employees to scan their fingerprints. The Seventh Circuit found that BIPA was preempted by Section 301 of the Labor Management and Relations Act because the claims were covered by a collective bargaining agreement and thus the class action claims could not be pursued by plaintiffs in federal court.

**Fox v. Dakkota Integrated Systems, LLC, 980 F.3d 1146 (7<sup>th</sup> Circ. 2020) (BIPA, Article III).**

Fox accused Dakkota “of violating the full range of its Section 15(a) duties,” requiring entities to develop, publicly disclose, and comply with data retention schedules and destruction guidelines, and said those violations led to the unlawful retention and sharing of her handprint after her employment ended with a third-party database administrator. The Seventh Circuit found that this did constitute an “injury in fact” sufficient to confer Article III standing because the unlawful retention constituted “a concrete and particularized invasion of [the plaintiff’s] privacy interest in her biometric data.”

**Gardiner v. Walmart, Inc., 20-cv-04618-JSW, 2021 U.S. Dist. Lexis 75079 (N.D. Cal. Mar. 5, 2021)(CCPA).** In a class action plagued by pleading errors, the trial court granted defendant’s motion to dismiss Plaintiff’s California Consumer Privacy Act (CCPA), negligence, unfair competition, and breach of contract claims for an alleged data breach of a retail website. The

plaintiff failed to identify any date on which the breach allegedly occurred. Because the CCPA applies only to data breaches occurring on or after January 1, 2020, and because the plaintiff failed to plead that the alleged breach occurred after this date, the court dismissed the plaintiff's CCPA claim. Further, the plaintiff failed to plead with any specificity what personal information was impacted in the alleged breach. As a result, the Court found that the plaintiff failed to establish that the affected personal information had lost value or that the plaintiff was subject to future risk of identity theft. Finally, the plaintiff's argument that he lost the benefit of the bargain of his purchases at the defendant's store could not be established because he failed to point to any contractual terms establishing a relationship between the parties. The court granted the defendant's motion to dismiss with leave for the plaintiff to amend.

**Gil v. Winn-Dixie Stores, Inc., 993 F.3d 1266 (11th Cir. 2021)(website accessibility).** In a case filed by a blind customer against Winn Dixie, a grocery store and pharmacy chain, the Eleventh Circuit held that a website does not constitute a public accommodation for purposes of Title III of the Americans with Disability Act. Acknowledging a circuit split on the issue, the Eleventh Circuit relied on a plain reading of the Act to find that the term public accommodation refers exclusively to tangible physical locations. It further held that regardless of whether the website was a place of public accommodation under the Act, a website's incompatibility with a screen reading software did not constitute an intangible barrier to the blind customer's ability to access and enjoy the physical grocery store where the website does not include a point of sale system and all interactions initiated on the website must be completed in the physical store, which was physically accessible to the plaintiff.

**Goldstein v. Costco Wholesale Corp., 21-CV-80601-RAR, 2021 U.S. Dist. LEXIS 170815 (S.D. Fl. Sept. 9, 2021)(ECPA, FSCA).** Plaintiffs in a class action lawsuit alleged that defendant's use of "session replay" software that recorded mouse movements, clicks, session durations, search terms, and other information while plaintiffs used defendant's website violated the Florida Security of Communications Act (FSCA). The Florida court rejected this argument, holding that the information collected fell outside of the FSCA's scope because the recordings of plaintiff's purported communications contained no substance. The court analogized to the FSCA's "federal counterpart, the Electronic Communications Privacy Act" (ECPA). The ECPA distinguishes between a "record" or other information pertaining to a customer, and "the contents – i.e., substance, purport, or meaning – of the communication itself." A record, such as dialing, routing, addressing, or signaling information, does not constitute "contents" for purposes of the ECPA. The court reasoned that the session replay recordings of mouse clicks and search terms at issue were akin to record information because they were the signals of how the communication was transmitted. Therefore, they cannot be considered "contents" as required by the FSCA because they did not shed light on the substance of the communication. The court further found that the FSCA specifically exempts "any communication from an electronic or mechanical device which permits the tracking of the movement of a person or an object," such as a hidden security camera. The court found that the session replay software at issue functioned more like a security camera that tracked movement than a device shedding light on the content of

a communication. Finally, the court acknowledged that the defendant had raised additional arguments that would likely be meritorious, including consent. But, the court found it unnecessary to consider these arguments because the defendant's "recordings of [p]laintiff's purported communications contained no substance. No substance means no contents, no contents means no interception, and no interception means no FSCA violation."

**Guo Wengui v. Clark Hill PLC, No. 19-3195, 2021 WL 106417 (D.D.C. Jan. 12, 2021)(attorney-client privilege in data breach context).** The plaintiff in this action sued his former law firm for alleged damages resulting from a data breach. The defendant law firm claimed that reports on the data breach generated by an outside data security consultant were privileged attorney-client communication and protected work product and pointed to the fact that it had a different data security consultant on retainer for routine data incident investigations and "continuity of business" recommendations, and that the second firm was hired by, and reported to, their outside counsel. But the court disagreed, noting that the consultants on retainer had essentially stepped aside and performed no work related to this incident, and that the second data security consultant's role appeared "far broader than merely assisting outside counsel in preparation of litigation." The report contained findings and recommendations for improving the law firm's overall cybersecurity framework and was distributed to non-lawyers, including IT personnel, leading to the court's conclusion that the new firm was hired to work on this incident more as a test of their expertise and capabilities than in anticipation of litigation.

**In re: Blackbaud, Inc., No. 2972, 2021 U.S. Dist. Lexis 151831 (D.S.C. Aug. 12, 2021)(CIMA).** In a multidistrict consolidated action stemming from a ransomware attack, the United States District Court for the District of South Carolina found that a cloud software provider may qualify as a medical provider handling medical information for purposes of California Confidentiality of Medical Information Act (CMIA) claims even where there is no direct contractual relationship between the service provider and the data subject. The court rejected Blackbaud's arguments that no California plaintiff had purchased any product directly from Blackbaud and that the plaintiffs had failed to allege that Blackbaud collected information for medical purposes. Instead, the Court held that the CMIA applies to entities "that are not ordinarily considered medical providers, such as technology companies that process and maintain medical information" on behalf of third party businesses. Direct product or service offerings are not required and the CMIA applies to businesses that maintain medical information, regardless of whether that is the primary purpose of the business.

**In re Capital One Consumer Data Sec. Breach Litig., No. 1:19-md-2915, 2020 WL 2731238 (E.D. Va. May 26, 2020), *aff'd*, 2020 WL 3470261 (E.D. Va. June 25, 2020)(attorney-client privilege).** In this data breach case, the plaintiffs moved to compel the production of reports provided to the defendant by an outside data security consultant, Mandiant. The court found that

the reports were not protected as attorney work product, as the defendant had a standing relationship with Mandiant to produce periodic assessments of the defendant's data security. The only difference between the reports in question and prior reports were that the agreement was modified to state that Mandiant was acting under the defendant's outside counsel's supervision and reporting to outside counsel. However, all the other terms of service were the same, and the reports regarding the instant incident were distributed as in the usual course of business to 50 employees of the defendant, four government agencies, the defendant's accounting firm, and the "corporate governance general email box." In addition, the retainer payment was designated as a business expense and did not come out of the legal department budget. The court applied the "because of" test to determine whether the documents sought were generated in anticipation of litigation, and the "driving force" test to determine whether the report would have been essentially the same whether or not litigation was anticipated. The Magistrate Judge found that under both tests, work product protection was unavailable, and the trial court upheld this holding on appeal.

In subsequent unpublished decisions in this same case, the Magistrate Judge declined to compel production of a "root cause analysis" report prepared by PricewaterhouseCoopers ("PwC") finding that the "driving force" behind commissioning the report was litigation defense and therefore protected under the work product doctrine, its subsequent use for remedial purposes notwithstanding. On appeal to the trial court, the Magistrate Judge's decisions were affirmed.

**In re Dominion Dental Services U.S.A., Inc. Data Breach Litigation, 429 F.Supp.3d 190 (E.D. Va. 2019) (attorney-client privilege in data breach context).** This class action arose out of the discovery of a nearly decade-long pattern of unauthorized access to dental patients' financial and medical information. The plaintiffs moved to compel production of a report produced by cybersecurity firm Mandiant in the wake of the data breach. Applying the "driving force" test for work product protection, the court found that Mandiant had been retained nearly a year before the breach was discovered, well before litigation stemming from that breach could have been anticipated, and that the resulting reports were used for non-litigation purposes. Most notably, the defendant distributed a statement to its client insurance firm stating, "we are still investigating this with the assistance of FireEye Mandiant, a world leading cybersecurity firm," and instructed the firm to "assure their own customers that Dominion brought in Mandiant to assist in the investigation." The fact that a separate retention agreement was executed once litigation was reasonably anticipated that expressly incorporated counsel in the direction of the work was not controlling, and the subsequent agreement was identical in nearly every other respect with the prior agreement. In the words of the court, "[t]he addition of language referencing 'under the direction of Counsel' appears to be designed to help shield material from disclosure rather than to fundamentally alter the business purposes of the work."

**In re Rutter's Data Security Breach Litigation, No. 1:20-CV-382, 2021 WL 3733137 (M.D. Pa. July 22, 2021)(attorney-client privilege in data breach context).** In May of 2019, the



Rutter's convenience store chain corporate office received alerts from Carbon Black Defense which "detail[ed] the execution of suspicious scripts and indications of the use of potentially compromised credentials." The firm immediately hired outside counsel, and in turn, outside counsel hired Kroll "to conduct forensic analyses on Rutter's card environment and determine the character and scope of the incident." The investigation took two months and included numerous communications between Kroll and Rutter's. Kroll provided Rutter's with a written report at the conclusion of the investigation, and Rutter's paid Kroll directly, as revealed in a later Fed. R. Civ. P. 30(b)(6) deposition of Rutter's Vice President of Technology, taken by plaintiffs in the subsequent class action lawsuit. Rutter's objected to discovery of the communications, claiming both attorney work product protection and attorney-client communication privilege. The court found that the Kroll report was not commissioned to prepare for litigation, pointing to the plain language of the "Description of Services" section of the contract, which stated, "[t]he overall purpose of this investigation will be to determine whether unauthorized activity within the Rutter's systems environment resulted in the compromise of sensitive data, and to determine the scope of such a compromise if it occurred." In addition, the corporate deponent, who signed the contract, testified that he was not contemplating litigation at the time and would have entered into the same arrangement whether or not lawsuits had been filed. The court concluded that attorney work product protection did not apply. Turning to the attorney-client privilege claim, the court found that even though Kroll was hired by Rutter's outside counsel, the scope of Kroll's work did not include "presenting [legal] opinions and setting forth ... tactics" but was limited to aiding Rutter's in identifying and remediating potential cyber liabilities.

**McCoy v. ALPHABET, Inc., 20-cv-05427-SVK, 2021 U.S. Dist. Lexis 24180 (N.D. Cal. Feb. 2, 2021) (California UCL, CCPA).** Defendant Google filed a motion to dismiss all claims in a class action alleging the unauthorized collection of usage statistics for third party applications on Android smartphones. The trial court rejected Google's fundamental argument that it had disclosed its data collection practices in its privacy policies and terms of use, which plaintiffs received and consented to. The court found that the policies, which stated that user "activity on third party sites and apps that use [Google's] services" would be collected and analyzed, was not sufficiently specific to support a motion to dismiss. Google bore the burden to establish the existence of consent, and the court found that it failed to demonstrate unambiguous clarity in the terms of its policies. As a result, the court refused to dismiss the plaintiff's claims for deceit and breach of contract. The court further upheld the plaintiff's unfair competition claims, declining to find that the "benefits from collecting that information to develop new products, features, and technologies for the benefit of the users and the public necessarily outweighs the harm" to consumer privacy. However, the court did dismiss plaintiff's claims for intrusion upon seclusion, noting that courts have "consistently refused to characterize the disclosure of common, basic, digital information to third parties as serious or egregious violations of social norms." It also dismissed plaintiff's claim under the California Consumer Privacy Act, as there was no breach required to establish a basis for the claim.

**McDonald v. Symphony Bronzeville Park, 2020 Ill. App (1st) 192398 (Ill. App. 2020) (BIPA, Workers Compensation bar).**

Defendant nursing home required an employee to provide her fingerprints for timekeeping purposes, allegedly without adhering to BIPA's consent and disclosure requirements. Defendant argued that the claims were barred by Illinois' Workers Compensation Statute ("WCA"). The appellate court found that BIPA's statutory and liquidated damages were not barred by the WCA because the WCA protects workers from actual injuries, and actual damages need not be suffered to bring an action under BIPA. Pending appeal in the Illinois Supreme Court.

**McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295 (2d Cir. 2021)(Article III standing).** In a class action involving the inadvertent sharing of employee personally identifiable information (PII), the Second Circuit considered whether a plaintiff may establish standing based on a risk of future identity theft or fraud stemming from a data breach. An employee of the defendant accidentally sent an email to all of the defendant's sixty-five employees containing a spreadsheet of present and past employee PII, including Social Security Numbers and other sensitive information. The parties conceded that there was "no evidence that any class members' identity was actually stolen . . . , let alone misused, and that the sharing of plaintiffs' PII was not the result of any intentional act by third parties such as hacking or some sort of criminal conduct from which it could be inferred that those who retained data intended to and were likely to misuse it." As a result, the district court determined that the plaintiffs lacked sufficient Article III standing. On appeal, the Second Circuit identified three factors that plaintiffs in data breach cases can use to establish Article III standing based on the fear of future identity theft resulting from a data breach: (1) whether the plaintiff's data was exposed; (2) whether other consumers' data that was also exposed has been misused; and (3) whether the data is sensitive and of a type likely to be misused. The Second Circuit rejected the contention that there is a "circuit court" split on the issue of whether fear of identity theft is sufficient to establish Article III standing. It found that no court had ever held that a plaintiff lacked standing where the plaintiff had adequately plead a substantial risk of identity theft. Additionally, the Court found that even de minimis time and money spent to protect against identity theft can establish standing where it is called for by a well pled substantial risk of identity theft. However, time and money spent to protect against identity theft where there is no substantial risk is akin to a self-inflicted injury and not sufficient to establish Article III standing. Applying the factors to the case at hand, the Second Circuit found that although the information was of the type that "might put the plaintiffs at a substantial risk of identity theft or fraud," plaintiffs "never alleged that their data was intentionally targeted" or that it "was in any way misused because of the accidental email." Therefore, the Court upheld the district court's dismissal of the complaint for failure to establish an Article III injury.

**Rahman v. Marriott Int’l, Inc., SA CV 20-00654, 2021 U.S. Dist. Lexis 15155 (C.D. Cal. Jan. 12, 2021) (CCPA, Article III standing).** The Central District of California dismissed a class action suit asserting claims for negligence and violation of the California Consumer Privacy Act (CCPA) for lack of Article III standing. The class was comprised of Marriott customers whose personal information was improperly accessed by Marriott employees in Russia. Marriott’s internal investigation confirmed that only names, addresses, phone numbers, email addresses, genders, birth dates, and loyalty account numbers were accessed without authorization. The district court found that the sensitivity of the personal information, combined with its theft, are prerequisites to finding that plaintiffs adequately alleged an injury in fact. “Without a hack of information such as social security numbers, account numbers, [passport information], or credit card numbers,” a plaintiff “has not suffered an injury in fact and cannot meet the constitutional requirements of standing.”

**Tims v. Black Horse Carriers, 2021 IL App (1st) 200563 (Ill. App. 2021) (BIPA, statute of limitations).**

The Illinois Appellate Court found that, although the BIPA is silent as to the applicable statute of limitations, claims brought under section 15(a), (b), and (e) of the statute, which requires companies to have a publicly available policy, obtain informed consent, and reasonably safeguard biometric data, are subject to a five (5) year limitations period. BIPA claims brought under sections 15(c) and (d) of the statute, which are claims that prohibit profiting from the use of biometric data or disclosure of biometric data are subject to a one (1) year statute of limitations. This is because each claim under BIPA is unique. And section 13-201 of the Illinois Code of Civil Procedure provides a one (1) year statute of limitations for “actions for slander, libel or for publication matter violating the right of privacy,” while section 13-205 has a five-year “catchall” statute of limitations for “all civil actions not otherwise provided for.” The court found that 13-201 only applies to privacy actions “where publication is an element or inherent part of the action.” Thus, section 13-201’s one (1) year statute of limitations only applies to BIPA claims under sections 15(c) and (d) of the statute, which prohibit entities from “sell[ing], lease[ing], trad[ing], or otherwise profit[ing] from” or disclosing biometric data because publication is included in the cause of action. Conversely, the court found that claims under sections 15(a), (b), and (e) do not have an element of publication or dissemination and thus, the five (5) year “catchall” statute of limitations applies.

**Thornley v. Clearview AI, Inc. 84 F.3d 1241 (7<sup>th</sup> Cir. 2021)(BIPA, Article III)**

In this case, plaintiffs alleged that Clearview violated BIPA § 15(c) (prohibiting entities from selling or otherwise profiting from biometric data). However, the Seventh Circuit found that plaintiffs had not “suffered any injury as a result of the violations” beyond the “statutory aggravement.” Because Plaintiffs had alleged only a bare procedural violation that did not qualify for Article III standing, the case was remanded to state court.

**TransUnion, LLC v. Ramirez, 141 S. Ct. 2190 (2021)(Article III standing).** Expanding on *Spokeo, Inc. v. Robins*, the Supreme Court raised the barrier for federal privacy actions by holding that a statutory violation without a showing of actualized concrete harm is not sufficient to establish standing under Article III. TransUnion, one of the “Big Three” credit reporting agencies, offered a credit checking service that compared the subject’s name to a Federal database of Americans who threaten national security. The service relied only on comparison of first and last name of the consumer to the federal database and frequently resulted in false positives. A class of 8,185 individuals who were improperly flagged by this system brought suit against TransUnion for failure to use reasonable procedures to ensure the accuracy of their credit files as required by the Fair Credit Reporting Act (FCRA). Of the 8,185 class members, only 1,853 actually had their reports disseminated to third parties. The remaining 6,332 members merely had flags placed on their accounts, which were not disclosed to third parties. The Ninth Circuit affirmed a jury award for all class members, reducing a \$60M award of statutory and punitive damages to roughly \$40M. The Supreme Court affirmed the ruling to the 1,853 members, finding that the publication of false information about the consumers when their credit checks were performed was akin to the common law tort of defamation. But it reversed and remanded for the remaining 6,332 members who alleged only violations of the FCRA. These plaintiffs – who could not rely on defamation – advanced “a separate argument based on the asserted risk of future harm”, arguing that the existence of misleading alerts in TransUnion’s internal credit files exposed them to a material risk that the information would be disseminated in the future, thereby causing harm. The Court rejected this argument, finding that while imminent future harm may be sufficient to warrant injunctive relief, it is not sufficient in this case to warrant damages. The Court reasoned that “if the risk of future harm materializes and the individual suffers a concrete harm, then the harm itself, and not the preexisting risk, will constitute a basis for the person’s injury and for damages. If the risk of future harm does not materialize, then the individual cannot establish a concrete harm sufficient for standing.” Borrowing the defendant’s analogy of driving near a drunk driver, the Court found that a lack of injury would typically be “cause for celebration, not a lawsuit.” Finally, the Court highlighted that many of the plaintiffs did not know that there were alerts in their credit files and would not be made aware until they received a check in the mail for their supposed injuries. Justice Kavanaugh stated that it “is difficult to see how a risk of future harm could supply the basis for a plaintiff’s standing when the plaintiff did not even know that there was a risk of future harm.” Therefore, the Court rejected the plaintiffs’ argument based on the risk of future harm, holding that “the mere existence of inaccurate information in a database,” a statutory violation without a showing of concrete harm, “is insufficient to confer Article III standing.”

**Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332 (11th Cir. 2021)(Article III standing).** In this case, a plaintiff brought suit on behalf of a putative class of customers seeking damages relating to his loss of credit card rewards points, loss of use of his card, and lost time and costs associated with cancelling his card and protecting against future identity theft. The Eleventh Circuit found that without specific evidence of some misuse of class members’ data, a named plaintiff will struggle to plead sufficient factual allegations to show that the threatened

harm of future identity theft was “certainly impending” or that there was a “substantial risk” of such harm. The Eleventh Circuit also found that where there is no substantial risk of future identity theft, purported mitigation efforts following a breach are self-inflicted injuries not sufficient to establish Article III standing.

**Vance v. Microsoft, 2021 U.S. Dist. LEXIS 48350, (W.D. Wash, March 15, 2021) (BIPA).**

In this case, the Western District of Washington found that Microsoft Corp. did not violate BIPA’s prohibition on selling, leasing, trading, or otherwise profiting from a person’s biometric information. The court held that “§ 15(c) regulates transactions with two components: (1) access to biometric data is shared or given to another; and (2) in return for that access, the entity receives something of value.” The court indicated that “the biometric data may be so integrated into a product that consumers necessarily gain access to biometric data by using the product or service.” The court found that while Microsoft used biometric data to “improve its facial recognition products and technologies,” which improved the products’ effectiveness and made them more commercially valuable, the allegations did not establish that Microsoft disseminated or shared access to biometric data to directly profit.

**Vance v. Amazon, 2021 U.S. Dist. LEXIS 48433 (W.D. Wash., March 15, 2021) (BIPA).**

In contrast to *Vance v. Microsoft*, the Western District of Washington court found (on a motion to dismiss) that plaintiff had stated a viable claim that Amazon.com Inc. violated Section 15(c) of BIPA because its software allowed “users to match new images of faces with existing, known facial images ‘based on their visual geometry,’” which supported the “reasonable inference that selling Amazon’s products necessarily shares access to the underlying biometric data in exchange for some benefit to Amazon.”

**Van Buren v. United States, 141 S. Ct. 1648 (2021) (CFAA).**

Reversal of 11th Circuit finding that police officer Nathan Van Buren violated the Computer Fraud and Abuse Act (CFAA) when he accessed a law enforcement database to retrieve information about a particular license plate number in exchange for money, which was a violation of a department policy. The CFAA subjects to criminal liability anyone who “intentionally accesses a computer without authorization or exceeds authorized access.” The term “exceeds authorized access” is defined to mean “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.” A jury convicted Van Buren, and the District Court sentenced him to 18 months in prison. Van Buren appealed to the Eleventh Circuit, arguing that the “exceeds authorized access” clause applies only to those who obtain information to which their computer access does not extend, not to those who misuse access that they otherwise have. The Eleventh Circuit held that Van Buren had violated the CFAA. The Supreme Court disagreed and found

that “an individual ‘exceeds authorized access’ when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him.” However, because Van Buren had authorized access to the license plate database, he did not exceed authorized access “even though he obtained information from the database for an improper purpose.”