Articles + Publications | March 2022

More Privacy, Please – March 2022

WRITTEN BY

Molly S. DiRago | Ronald Raether, Jr. | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | Robyn W. Lin | Lissette Payne | Jonathan "Grady" Howe | Kamran Salour

Editor's Note: It may be the shortest month of the year, but February 2022 saw a flurry of privacy — especially biometric — legislation move closer to enactment. Kentucky, California, Maryland, and New York state introduced biometric-focused laws, each largely mirroring Illinois' Biometric Information Privacy Act (BIPA) and each containing a private right of action. Maine, Utah, and Florida introduced comprehensive privacy bills, and Iowa's and Oklahoma's inched closer to enactment by passing committees. On the litigation front, Texas brought claims against Facebook under its rarely invoked Capture or Use of Biometric Identifier Act (CUBI), which allows enforcement only by the attorney general, and thus, has not seen the onslaught of litigation seen by BIPA. Additionally, courts continue to embolden BIPA plaintiffs, as three new rulings broadened its reach: *In re: Clearview AI, Inc. Consumer Privacy Litigation*, where the Northern District of Illinois rejected arguments that BIPA violated First Amendment rights; *McDonald v. Symphony Bronzeville Park LLC*, in which the Illinois Supreme Court held that the Workers' Compensation Act did not bar BIPA claims; and *Mosby et al. v. Ingalls Memorial Hospital et al.*, in which an Illinois appellate court held biometric information collected by a health care employer from its employees did not fall within BIPA's health care information exclusion. Internationally, the biggest headline covered the U.K.'s release of two new mechanisms to effectuate cross-border transfers of data, which provide more uniformity and clarity for U.K. GDPR compliance.

US Laws and Regulation

- **California Proposes Biometric-Focused Privacy Law.** California joined the ranks of states that have introduced biometric-focused privacy acts. On February 17, Senator Bob Wieckowski (D-CA) introduced SB-1189, which mirrors BIPA by imposing requirements on private entities that possess biometric information to develop and make available a written policy, establishing a retention schedule and guidelines for permanently destroying the biometric information. Like BIPA, it also includes a private right of action for individuals to pursue a civil action. Note that the California Consumer Privacy Act (CCPA) already includes biometric information in its definition of personal information and provides for a private right of action, but only in certain limited circumstances. SB-1189 would provide for statutory damages of $100 to $1,000 per violation, per day or actual damages.

- **Maryland Launches New Biometric Law.** Maryland introduced its own biometric law, HB 259, titled the "Biometric Identifiers Privacy Act." Like other biometric laws, including BIPA and Kentucky, this bill would require companies to obtain consent before collecting biometric information, inform consumers what information is being collected, and provide a retention schedule. It also would prohibit businesses from profiting from consumers' biometric information. Per the new trend, Maryland's new biometric law includes a private right of

©2026 Troutman Pepper Locke

action. Furthermore, HB 259 provides for actual damages or statutory damages in the amount of $1,000 for negligent violations or $5,000 for intentional or reckless violations.

- **New York Re-Introduces Biometric Privacy Law for Fourth Time.** For the fourth time since 2018, New York lawmakers introduced Assembly Bill A27, the "Biometric Privacy Act." The bill would apply to two types of information: biometric identifiers and biometric information. Biometric identifiers include retina or iris scans, fingerprints, voiceprints, or hand or face geometry. In comparison, biometric information denotes biometric identifiers used to identify an individual. The bill would prohibit businesses from profiting from biometric information, including the sale, lease, or trade of biometric identifiers or biometric information. It also would impose notice and consent obligations before the collection of biometric data. Like other biometric laws, it would provide consumers with an individual right of action with the potential to obtain damages, attorneys' fees, and injunctive relief. Like Illinois' BIPA, a negligent violation could result in liquidated damages of $1,000, and intentional or reckless violations could result in liquidated damages of $5,000.

- **Maine Initiates Comprehensive Privacy Law.** On February 16, Maine Senator Joseph Rafferty (D-ME) introduced an act to protect consumers' privacy by giving them greater control of their data and to establish consumer protections for small-dollar loans. Referred to the Innovation, Development, Economic Advancement, and Business Committee, the bill would provide consumer rights, including a right to request information, delete personal information, and opt out of the sale of personal information. No private right of action exists under this bill. Statutory damages under this bill include a civil penalty of not more than $2,500 per violation or $7,500 for each intentional violation.

- **Utah's Comprehensive Privacy Law Awaits Governor's Signature.** On February 25, the Utah Senate passed the Utah Consumer Privacy Act (UCPA), and the House unanimously passed the bill on March 2. The bill now awaits Governor Spencer Cox's signature. If signed, Utah would be the fourth state to pass a comprehensive privacy bill after California, Virginia, and Colorado. Unlike other state bills, the UCPA would create a split system where the Department of Commerce's Consumer Protection Office will consider and investigate claims, yet without having enforcement power. If there is substantial evidence of a violation, the attorney general's office can elect to pursue the claim. For further analysis, click here.

- **Florida Privacy Bill Establishes Tiered Approach to Controversial Private Right of Action.** Florida Representative Fiona McFarland (R-FL) reintroduced comprehensive privacy bill House Bill 9, which controversially contains a private right of action. Previously, the Florida Senate sought to avoid a private right of action in any enacted privacy bill, while its House supported it. Currently, McFarland's House bill — containing the private right of action — is the only bill gaining traction. To address the political division regarding the private right of action, the bill establishes a unique tiered approach not seen in other state privacy proposals, whereby the private right of action and attorneys' fees are only available depending on the defendant's earnings level. Specifically, there would be no private right of action available against businesses earning $50 million or less, but private enforcement would still be applicable. For businesses earning between $50 million and $500 million, the private right of action is available, but recovery of attorneys' fees is not. Finally, for businesses reaping over

$500 million in revenue, both a private right of action and attorneys' fees recovery are available. The new revised bill also adds a one-year statute of limitation after discovery of a violation and moves the effective date from January 1, 2023 to July 1, 2023. HB-9 was officially "indefinitely postponed and withdrawn from consideration," on March 12th and the Florida's legislative session ended on March 14th.

- **Iowa's Comprehensive Privacy Bill Moves From Committee to House Floor.** The Iowa House Information Technology Committee voted 15-0 to advance House Study Bill 674, which introduces consumer data rights, including the right of correction, the right to request information, opt out, and deletion. It also contains exclusive attorney general enforcement and a 30-day cure period. Now eligible for a full house vote, if passed, it would take effect January 1, 2024. Controllers or processors found in violation face a penalty of up to $7,500 per violation.

- **Oklahoma Computer Data Privacy Act Inches Closer to Enactment.** The Oklahoma House Technology Committee passed House Bill 2969 on a 6-0 vote. The bill will now move to the House floor for a third reading and potential passage out of chambers. The bill provides for consumer rights including the right of deletion, prohibition of retention of data, and access. Violators of the act face a fine of up to $2,500 per violation or $7,500 per intentional violation.

US Litigation and Enforcement

- **Texas AG Sues Facebook Parent, Meta Platforms.** In one of the first-ever actions to enforce its CUBI, Texas Attorney General Ken Paxton sued Meta on February 14, alleging the Facebook parent illegally collected users' biometric data without their consent. The allegations mimic those in the consolidated action, *In re Facebook Biometric Information Privacy Litigation*, which asserts claims under Illinois' BIPA and recently resulted in a $650 million settlement. CUBI is similar to BIPA in that it (1) requires businesses to obtain users' informed consent before collecting their biometric data, (2) mandates destruction of the data in a reasonable time, and (3) prohibits selling, leasing, or otherwise disclosing the data except in limited circumstances. Unlike BIPA, however, CUBI does not have a private right of action component and can only be enforced by the Texas AG.

- **Illinois Court Rejects Clearview AI's Argument.** On February 14, a Northern District of Illinois judge rejected Clearview AI's arguments that Illinois' BIPA violates the First Amendment. In *In re: Clearview AI, Inc. Consumer Privacy Litigation*, Clearview AI currently faces a multidistrict litigation class action over allegations it covertly scraped over three billion photographs of facial images from the internet. The court held that the additional conduct of scrapping photographs from the internet "presents grave and immediate danger to privacy, individual autonomy, and liberty." A more detailed analysis can be found here.

- **Illinois Supreme Court Rules on Workers' Compensation Act and BIPA.** On February 3, the Illinois Supreme Court held the Workers' Compensation Act did not preempt BIPA damages. The Supreme Court held that plaintiff McDonald's injury involved the loss of her ability to maintain her privacy, which is neither a

psychological nor physical injury and therefore not compensable under the Workers' Compensation Act. The Workers Compensation Act awards damages according to a predetermined fee schedule, which eliminates variability in the value of each judgment. In comparison, BIPA awards the greater of actual or liquidated damages of $1,000 (for negligent violations) or $5,000 (for intentional or reckless violations). Read Troutman Pepper's analysis here.

- **Facebook Settles Class Action for $90M.** Facebook filed a proposed settlement, hoping to settle a class-action lawsuit that alleges Facebook collected its users' data when they visited websites with the Facebook "Like" button, even after they logged out of Facebook, despite telling users that it would not track their online activity after they logged out. Facebook then allegedly sold this impermissibly collected data and used the data to benefit themselves. Under the proposed settlement, Facebook would create a settlement fund of $90,000,000 and would delete all impermissibly collected data. If accepted, the settlement would resolve over a decade of litigation involving Facebook's alleged behavior and would fall in the top 10 largest privacy-based, class-action settlements in U.S. history.

- **FTC, WW International, and Kurbo Settle COPPA Violations for $1.5M.** WW International, Inc. (WW), formerly Weight Watchers International, Inc., and its subsidiary Kurbo, Inc. filed a proposed settlement with the Federal Trade Commission (FTC) for Kurbo by WW data collection practices, a child and teen weight loss program. In the FTC complaint, WW was accused of retaining the data of thousands of children indefinitely, without providing notice or receiving parental consent, in violation of the Children's Online Privacy Protection Act (COPPA) and Section 5 of the FTC Act. The proposed settlement requires WW to (1) delete all retained information that violated COPPA (as well as delete all algorithms and models based in any part on the information collected/retained in violation of COPPA); (2) pay a $1,500,000 penalty; (3) establish the procedures and policies necessary for COPPA compliance; and (4) maintain compliance reporting for 10 years.

- **California Attorney General Focuses on CCPA Implications of Consumer Loyalty Programs.** In recent statements, the California Attorney General, Rob Bonta, whose office is currently in charge of enforcing the CCPA has, in recent statements, noted that attention is on the privacy compliance of consumer loyalty programs. The California Attorney General's office has sent letters of noncompliance with the CCPA to major corporations in the retail, home improvement, travel, and food services industries for not providing a notice of financial incentive before consumers began participating in their loyalty programs that exchange a benefit for consumers' personal information. Pursuant to the CCPA, companies that offer a financial incentive in exchange for personal information must provide a notice of financial incentive before consumers opt into the program. Companies that receive a letter of noncompliance currently have 30 days to cure their violations.

- **Illinois Appellate Court Rules Health Care Employees Not Excluded From BIPA.** An Illinois appellate court recently held in *Mosby et al. v. Ingalls Memorial Hospital et al.* that fingerprint scans collected by a health care employer from its employees does not fall within a BIPA exclusion. The Section 10 exclusion provides, "biometric identifiers do not include information captured from a patient in a health care setting or information collected, used or stored for health care treatment, payment, or operations under the federal Health Insurance

Portability and Accountability Act of 1996 (HIPAA). Lead plaintiff Mosby had argued she was required to scan her fingerprint to gain access to a medication dispensing system. The court rejected the defendants' position to hold that the exemption at Section 10 only applies to information protected "under HIPAA," which the court stated is limited to patient information, not employees.

International Regulation and Enforcement

- **UK Releases Three New Documents Clarifying International Data Transfers.** On January 28, the United Kingdom's (U.K.) secretary of state for digital, culture, media, and sport presented the U.K. Parliament with two new mechanisms to effectuate cross-border transfers of data: (1) the International Data Transfer Agreement (IDTA) and (2) the international data transfer addendum to the European Commission's standard contractual clauses (SCCs) (Addendum). Any cross-border transfer of data from the U.K. to a third country restricted by U.K. GDPR Chapter V needs an appropriate transfer mechanism, such as executing the IDTA or the Addendum. The new IDTA is comparable to the EU's SCCs and includes four parts containing tables and mandatory clauses, while also meant to supplement the terms of a transfer agreement already using the new EU's SCCs. Barring any objections from the U.K. Parliament, these documents will become effective on March 21. The IDTA and the Addendum can be used immediately, and any contracts entered into on or before September 21, 2021 that uses the transitional standard clauses will remain adequate until March 21, 2024, in which either the IDTA or the Addendum will need to be adopted. To read more about the substantive aspects of the IDTA and the Addendum, please click here.

- **Ireland DPA Seeks Suspension of Data Transfers Against Meta.** Facebook owner Meta faces an imminent order from Ireland's data regulator to suspend data transfers to the United States. The case originated in a complaint by privacy campaigner Max Schrems, who argued European citizens' data is at risk when it is transferred to the U.S. Meta has 28 days to make submissions to this preliminary decision.

- **Big Fines Not a Measure of GDPR Success According to Irish Regulator.** Irish Data Protection Commissioner Helen Dixon claimed in a recent annual report that her office gained "significant momentum" in its GDPR enforcement efforts in recent months. The Irish authority faces continual criticism from consumer advocates and others for failing to adequately address enforcement and fining powers on other tech giants with their main EU establishment in Ireland, such as Facebook, Google, Apple, Twitter, and Microsoft. Dixon fired back at such accusations by claiming that neither the number of cases nor the size of the fines are treated as the sole measure of success. Rather, Dixon claimed that proper metrics for the GDPR's success are "measurable changes in behavior on the part of controllers and real-life benefits for data subjects." Dixon also called for a set of metrics that could help assess performance in a more objective way.

- **France's Constitutional Council Declares Prior Version of Data Retention Law Unconstitutional**. According to a question of constitutionality in a decision recently issued by France's Constitutional Council, components of the country's data retention regime were deemed unconstitutional. The council held that retention of data resulted in an infringement of the right to respect for private life, as well as a breach of EU law.

The contested provisions dealt with the identification of users of electronic communications services and the location of their communication terminal equipment, technical equipment, and characteristics. The council also cited concerns with the date, time, and duration of the communications, as well as the identification data of their recipients.

- **French Privacy Regulator Rules Against Google Analytics.** In a February 10 decision, the French privacy regulator ruled that an unnamed website cannot use Google Analytics because it transfers personal data to the United States in violation of EU privacy law. This is the second time an EU regulator ruled against Google. The first occurred in January by the Austrian regulator. The French regulator stated the additional measures Google adopted were not sufficient to exclude the accessibility of this data for U.S. intelligence services.

Troutman Pepper Team Spotlight: Tambry Bradford

As a trial attorney, Los Angeles Partner Tambry Bradford helps public and private companies achieve favorable results when complex data privacy matters result in a class action. Currently, Tambry is defending a cloud software company in numerous actions relating to a ransomware attack that occurred in early 2020, including multidistrict litigation and state and federal regulatory inquiries.

Tambry's practice encompasses a wide range of complex commercial litigation matters involving claims of fraud, unfair competition, due process violations, contract disputes, and products liability. She represents individuals and public and private companies in state and federal courts throughout the country. Tambry has handled appeals in California state appellate courts and the Ninth Circuit.

As part of her commitment to promoting diversity, equity, and inclusion, Tambry serves as the firm's West Coast Recruiting Committee chair and as a Troutman Pepper Diversity and Inclusion Committee member. In her free time, Tambry focuses on her international travel bucket list. Her last check on that list was a trip to Australia and New Zealand.

Upcoming Webinars and Events

- **Incident Response – Breaking Down the Roles of the Insurer, Insured, and Counsel | Tuesday, March 22, 2022 | 3 – 4 p.m. ET**

  Many businesses have cyber insurance to cover themselves in the event of an incident. Fortunately for many of them, they may not have needed to use it — just yet. Join this panel presentation to learn how cyber insurance impacts an organization's incident response efforts. Panelists will address the role of carriers, outside counsel, and third-party vendors during a security incident, and how cyber insurance may (or may not) alter an organization's response. Key issues will include:

  - The role of insurance carriers during incident response.
  - Selection of outside counsel and third-party vendors: Can businesses rely on their trusted advisors or do carriers get the final say?
  - The obligations of outside counsel and third-party vendors to insurance carriers and the insured.
  - Privilege concerns when carriers are involved.

Troutman Pepper attorneys will be joined by Linda Comerford, the AVP of cyber services and incident response at AmTrust, and Kayla Barker, the director of incident response at Tetra Defense. To register, please click here.

Recent Troutman Pepper Publications

- **Wisconsin House Passes New Comprehensive Privacy Bill**
- **Valentine's Day Order Gives No Love to Clearview AI's First Amendment Arguments**
- **California Lawmakers Propose Two Bills to Exempt Employee and B2B Data From Scope of CPRA**
- **UK Releases Three New Documents Clarifying International Data Transfers**
- **No Pain No Gain – Magistrate Judge Recommends Dismissal of Data Breach Suit Where Medical Information Was at Issue**
- **Financial Crimes Enforcement Network Makes Ransomware a Priority**

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management

©2026 Troutman Pepper Locke