ALSTON & BIRD

NRF Privacy Working Group Meeting

February 3, 2021

Donald Houser, Alston & Bird LLP

NRF National Retail Federation

"Session Replay" Litigation

- **What is "Session Replay" Litigation?**
  - Many retailers work with analytics vendors that utilize software that monitors customer usage of the retailer's website.
  - Many, many legitimate and consumer-friendly uses of this software. For instance, this software allows retailers to spot quickly issues with the website and improve customer experience.
  - Recent explosion of class action lawsuits filed (almost entirely in California) alleging that the software constitutes a surveillance device and that the software illegally "intercepts" customer communications.
- **25+ Class Action Lawsuits Filed in 2020**
  - *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (petition for writ of certiorari filed).
  - Most of these lawsuits were filed in the second half of 2020, i.e., post-*Facebook.*
  - Most were filed by the same Plaintiffs' firm, Bursor Fisher.
  - Defendants include Pacific Gas and Electric, Mazda, Blizzard Entertainment, Apple, Nike, and the list goes on.
  - Third-party vendors named as defendants include Mouseflow, Full Story, Miniclip, and Quantum Metrics.

"Session Replay" Litigation/ Claims Asserted

- **Core Claim Asserted – Violation of California's Invasion of Privacy Act ("CIPA")**
  - California's anti-wiretapping and anti-eavesdropping statute – designed "to protect the right of privacy."
    - Prohibits using a "machine, instrument, or contrivance" to make an "unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument," and through that connection, obtain the "contents of the communication." Section 631.
    - Prohibits using a device to "eavesdrop" on "confidential communications." Section 632.
    - Prohibits intentionally "manufacturing, assembling, selling, offering for sale, . . . possessing, transporting, and/or furnishing a wiretap device." Section 635.
    - Provides that a civil lawsuit may be brought by "any person who has been injured by a violation of this chapter," and that person may bring an action against the person who committed the violation for the greater of "either (1) $5,000" or "three times the amount of actual damages, if any sustained by the plaintiff." Section 637.

"Session Replay" Litigation/ Key Issues

- **Key Issues**
  - Section 631:
    - What about the fact that the retailer is a party to the communication with the customer? Can you really illegally intercept your own communication?
      - *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020).
      - *Membrila v. Receivables Performance Mgmt., LLC*, 2010 WL 1407274 (S.D. Cal. Apr. 6, 2010) (explaining that Section 631 applies "only to eavesdropping by a third-party and not to recording by a participant to a conversation").
    - What about the substance of the information acquired? Do mouse movements and clicks, IP addresses, and URL and similar information constitute the "content" of a communication?
      - In re *Zynga Privacy Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014) (explaining that divulging "identification and address information contained in a referrer header" as well as "record information" are not the contends of a communication under the analogous federal wiretap act).

"Session Replay" Litigation/ Key Issues

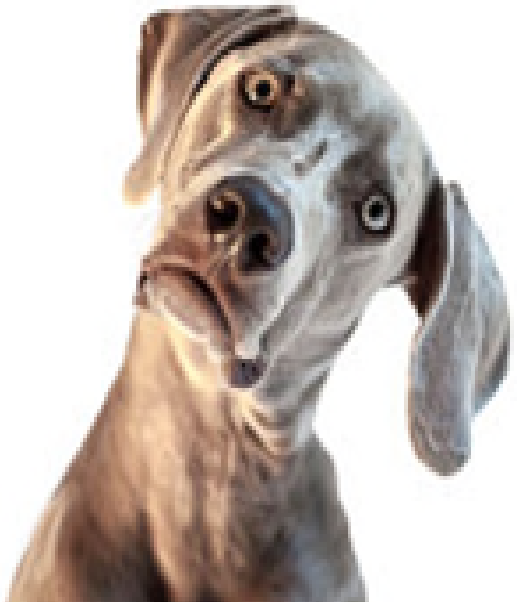
- **Key Issues**
  - Section 632
    - Assuming that a consumer is deemed to be communicating via a website, is that communication a "confidential communication" triggering liability under Section 632?
      - California courts have generally found that internet-based communications are not 'confidential' within the meaning of section 632 . . . ." *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836 (N.D. Cal.)
  - Section 635
    - Does contracting for the use of this type of software trigger liability?
      - *In re Lenovo Adware Litig.*, 2016 WL 6277245, at *7 (N.D. Cal. Oct. 27, 2016) (finding that mere possession of a wiretapping device is insufficient to give rise to liability under the federal wiretap act)
  - On the Horizon/ Cases to Watch
    - *Revitch v. New Moosejaw, LLC and Navistone, Inc.*, 18-cv-6827 (N.D. Cal.)

Illinois Biometric Information Privacy Act

- **BIPA**
  - Enacted in 2008 by the Illinois legislature; spurred by bankruptcy of Pay by Touch
  - Resulted in wave of litigation starting in ~2015/2016
    - Statutory damages and attorneys' fees
- **Who is Covered by BIPA**
  - BIPA has a long reach
  - "**Private entity**" means any individual, partnership, corporation, limited liability company, association, or other group, however organized.

Illinois Biometric Information Privacy Act

- **What Does BIPA Do?**
  - Regulates private entities' use of both biometric identifiers and biometric information
  - "**Biometric identifier**" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.
  - "**Biometric information**" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.



Illinois Biometric Information Privacy Act

- **What Does BIPA Require?**
  - Before obtaining biometric information ("BI"), the entity must:
    - Inform the person in writing that (a) it is collecting or storing BI and (b) the time span and purpose for collecting, storing, and using BI; and
    - Obtain a written release (informed consent);
  - Have a public written policy made available to the public for retaining and destroying BI;
  - Not sell, lease, trade, or profit from BI;
  - Not disclose BI unless an individual gives informed consent or unless required under law, warrant, or subpoena; and
  - Exercise care in storing, transmitting, and protecting BI from disclosure.

Illinois Biometric Information Privacy Act

- **Damages**
  - "Any person aggrieved by a violation" of the BIPA "may recover for ***each violation***[.]"
  - $1,000 ($5,000 if intentional or reckless) per violation
  - How is this calculated?
    - What constitutes a "violation"? Is it each capture or each scan?
- **Statute of Limitations: 2 years (?)**
  - Depends on the nature of the injury alleged and damages sought
  - 2 year SOL applies to claims for (a) ***personal injury*** and (b) a ***statutory penalty***
  - 5 year catch-all SOL applies if no other statute applies
  - When does the SOL accrue?
    - *Cothron v. White Castle Sys., Inc.,* 2020 U.S. Dist. LEXIS 141391, at *17 (N.D. Ill. Aug. 7, 2020) (finding that for statute of limitations purposes, the cause of action accrues at every single scan).

Illinois Biometric Information Privacy Act

- **Calculating the Amount in Controversy for Removal**
  - *Fernandez v. Kerry, Inc.*, 2020 U.S. Dist. LEXIS 64070, at *9 (N.D. Ill. Apr. 10, 2020) (applying a per-scan calculation)
  - *Peatry v. Bimbo Bakeries USA, Inc.*, 393 F. Supp. 3d 766, 770 (N.D. Ill. 2019) ("[B]ecause [plaintiff] has not shown that it is legally impossible for her to recovery $5,000 per fingerprint scan, a position plaintiff should be loath to take in light of the undecided interpretation of BIPA's damages provision, the Court leaves that determination to another day. At this stage, such recovery, although uncertain, remains plausible based on [plaintiff's] allegations and an expansive reading of BIPA's damages provisions.")

Illinois Biometric Information Privacy Act

- **Standing to assert a BIPA claim**
  - Illinois Supreme Court
    - Actual Injury NOT Required
    - *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197 (Ill. 2019)
  - U.S Constitution/ Article III standing
    - *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1267 (9th Cir. 2019), cert. denied, 140 S. Ct. 937 (2020)
    - Held Plaintiffs had suffered sufficiently concrete injury to confer Article III standing

Facebook, Ill. Users Ink Record $550M Biometric Privacy Deal

Illinois Biometric Information Privacy Act/ Class Actions

- **Emerging BIPA Issues & Why it Matters Outside Illinois**
  - Facial recognition - *In re Clearview AI, Inc. Data* Litigation
    - Burke v. Clearview AI, Case No. 20-cv-0370 (S.D. Cal.).
    - Wave of lawsuits filed following a January 18, 2020 New York Times article regarding Clearview AI – "The article described a dystopian surveillance database, owned and operated by a private company and leased to the highest bidder." Hall et al. v. CDW Government LLC et al., Case No. 1:20-cv-00846 (N.D. Ill.), ECF No. 1, para. 1.
    - Parties seeking consolidated treatment through the MDL process; oral arguments set for December 3, 2020 before JPML.
  - Companies outside Illinois must understand BIPA and associated risks.
    - *Bray v. Lathem Time Co.*, Case No. 19-3157 (C.D. Ill. Mar. 27, 2020)
      - Plaintiff alleged that his employer required him to use a Lathem facial recognition device and that Lathem violated BIPA
      - Lathem is a *third-party technology vendor based in Georgia* that made a employee time-keeping device
      - Collected information without satisfying BIPA
      - Resolved on a personal jurisdiction motion but significant implications for companies located outside IL.

Illinois Biometric Information Privacy Act/ Class Actions

- **Emerging BIPA Issues & Why it Matters Outside Illinois**
  - Preemption
    - *Frisby v. Sky Chefs, Inc.*, Case No. 19 C 7989 (N.D. Ill.) (employees required to resolve BIPA challenge using grievance procedures in collective bargaining agreement)
  - Do you know what ***your vendor*** did last summer (in Illinois)?

Beyond BIPA/ City of Portland Ordinance 190114

- City of Portland prohibits the use of Face Recognition Technologies by private entities in places of public accommodation in the City ordinance
  - Ordinance passed September 9, 2020.
- Private Right of Action:
  - "Any person injured by a material violation of this Chapter by a Private Entity has a cause of action against the Private Entity in any court of competent jurisdiction for damages sustained as a result of the violation or $1,000 per day for each day of violation, whichever is greater and such other remedies as may be appropriate."

California Consumer Privacy Act/ Overview

- **Fact sheet**
  - Passed as part of a deal to avoid a similarly named ballot initiative from being added to the November 2018 ballot by an organization called Californians for Consumer Privacy.
  - Signed into law June 28, 2018.
  - Effective January 1, 2020.
  - Amendment signed by Governor Brown on September 23, 2018.
  - On August 14, 2020, the California Office of Administrative Law approved the California Office of the Attorney General's Finally CCPA regulations .

California Consumer Privacy Act/ Scope

The CCPA's Reach

(1) businesses doing business in the State of California;

(2) that collect personal information; and

(3) relating to California residents.

California Consumer Privacy Act/ Scope

The CCPA's Reach

- "Business" means:
  - Any for-profit business entity;
  - That collects consumers' personal information, or on the behalf of which such information is collected;
  - That alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information;
  - *That does business in the State of California* (any business worldwide);
  - And…

California Consumer Privacy Act/ Scope

- **Satisfies one or more of the following thresholds:**
  - Annual gross revenues exceeding $25 million;
  - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, *households, or devices; OR*
  - Derives 50 percent or more of its annual revenues from selling consumers' personal information.

California Consumer Privacy Act/ Scope

- But wait…CCPA also defines "Business" to include:
  - "Any entity that controls or is controlled by a business as defined" above and "that shares common branding with the business."
    - "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.
    - "Common branding" means a shared name, servicemark, or trademark.

California Consumer Privacy Act/ Scope

- **"Personal information" has an exceptionally broad scope.**
  - Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
  - Digital advertising and targeting profiles, web and mobile app browsing histories, and retail analytics profiles (e.g., in-store locations of mobile devices) are all potentially in scope.
  - Broader than the definition of personal information in California's data breach statute.

California Consumer Privacy Act/ Personal Information

- **In addition to the typical data types (e.g., name, address, social security number), the definition includes:**
  - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
  - Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
  - Biometric Information and geolocation data.
  - Audio, electronic, visual, thermal, olfactory, or similar information.
  - Inferences drawn from any of the identified information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

California Consumer Privacy Act/ Litigation Issues

- **Private Right of Action – Data Security Breach**
- Any consumer whose unencrypted or non-redacted personal information (as defined more narrowly in California's data security statute) is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the **duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information**
  - To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.
  - Injunctive or declaratory relief.
  - Any other relief the court deems proper.

California Consumer Privacy Act/ Class Actions

- **California's Unfair Competition Law – Is Every Violation of CCPA "Unlawful"?**
  - The California Unfair Competition Law (the "UCL") authorizes a private right of action for any unlawful or unfair business practice.
  - An exception applies when the law in question "*actually bar[s] the action.*"
  - The CCPA states that "nothing in this [statute] shall be interpreted to serve as the basis for a private right of action under any other law."
  - *Does this "actually bar the action"? Why didn't the legislature affirmatively preclude an action under the UCL?*
  - Examples:
    - The CCPA "notice at collection" is not academic – it's a real and significant litigation risk. *See, e.g.*, *Cullen v. Zoom Video Comms., Inc.*, No. 5:20-cv-2155, Dkt. No. 1 (N.D. Cal. filed Mar. 30, 2020) (alleging Zoom violated CCPA because it "collected [users'] personal information as defined in the CCPA and failed to inform [them] of the same at or before the point of collection")

California Consumer Privacy Act/ Class Action Litigation Issues

- **Invasion of Privacy?**
  - Can a violation of the CCPA serve as a predicate for an invasion of privacy claim?
- **First competitor-vs-competitor UCL case on the basis of CCPA violations**
  - *Bombora v. ZoomInfoData*, Case No. 20-cv-365858 (Santa Clara Cty. Super. Ct.)
  - Bombora alleges ZoomInfo has a competing B2B analytics product that was built on top of CCPA-violative data practices → thus constitutes an unlaw/unfair practice under the UCL
  - Specifically, Bombora alleges ZoomInfo built an analytics product on top of personal information without (a) providing notices of collection under 100(b) CCPA, or (b) providing notices of data sales and an opt-out.
- **Personal Jurisdiction?**
- **Arbitration?**
  - Cal Civ. Code § 1798.192: "[A]ny provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under [the CCPA], including, but not limited to, any right to a remedy or means of enforcement" is "void and unenforceable."