Reimagining Data Privacy Litigation:
How Plaintiffs Apply Old Laws to New Enterprises

ACC/DFW

March 7, 2024

Samir Bhavsar & Nick Palmieri, Baker Botts LLP

BAKER BOTTS

Table of Contents

VIDEO PRIVACY PROTECTION ACT 01

VPPA

BAKER BOTTS

Video Privacy Protection Act

Intent	Prevent disclosure of video-rental histories related to a specific person
Actual	Pursuing companies that utilize third-party cookies on their website or through their services

1988

VPPA Passed
- Response to release of Robert Bork's video rental history
- Directed towards "video tape servicer providers" and their handling of "personally identifiable information"

2008

First major class action using VPPA
- Filed against Blockbuster for use of Facebook's "Beacon"
- Directed towards "video tape servicer providers" and their handling of "personally identifiable information"

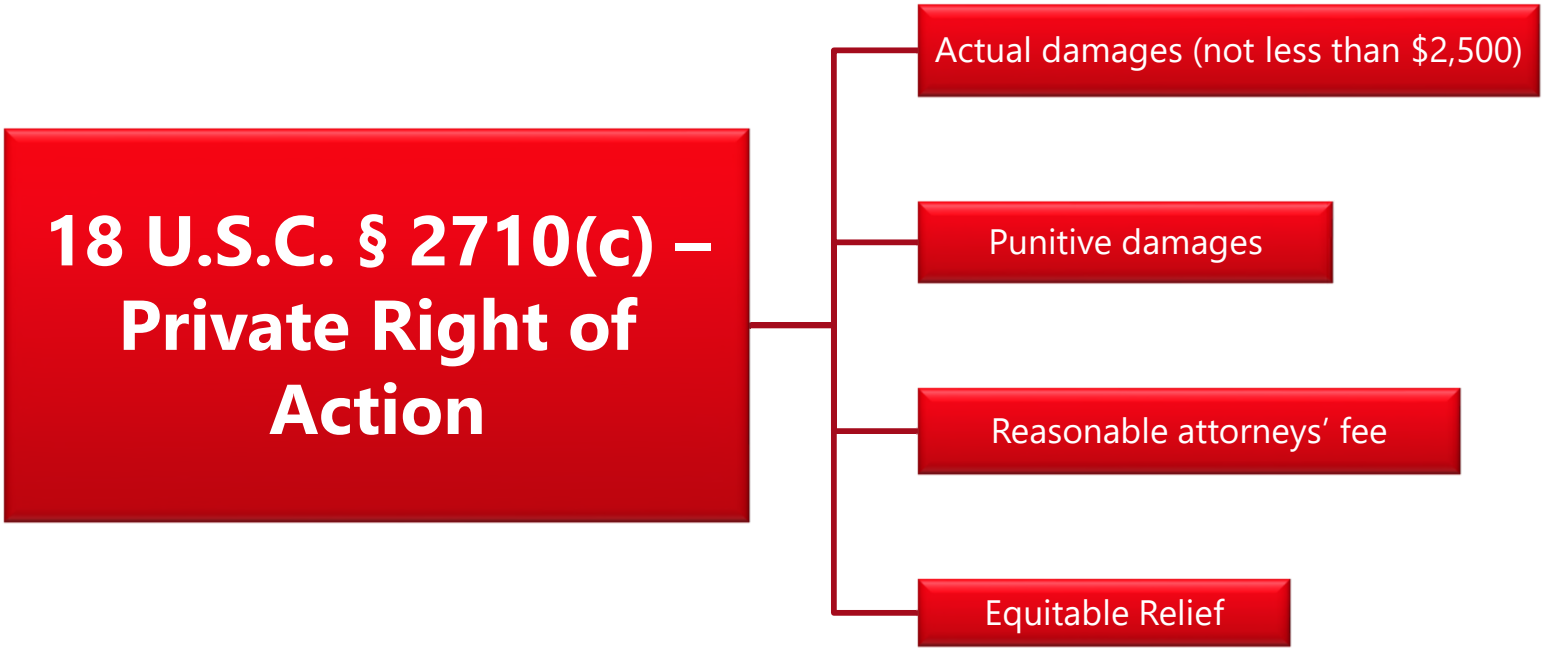
Key Definitions

"video tape service provider" – Any person engaged in . . . rental, sale, or delivery of prerecorded video cassette tapes *or similar audio visual materials*

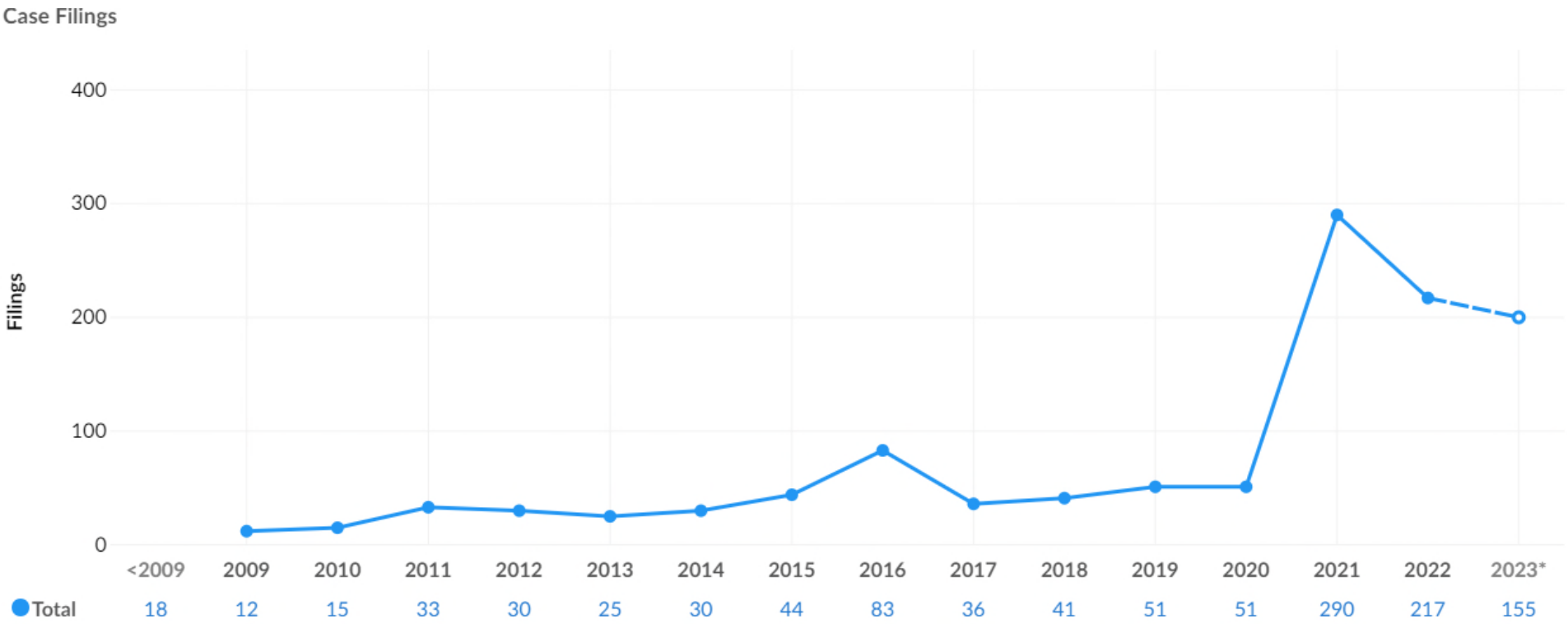
"personally identifiable information" – Information which identifies a person as having requested or obtained *specific video materials or services*

"consumer" - Any *renter, purchaser or subscriber* of goods or services from a video tape service provider

Causes of Action



Trend


Case Filings
Filings
400
300
200
100
0
<2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023*
Total
18
12
15
33
30
25
30
44
83
36
41
51
51
290
217
155

Profile of a Defendant

Online presence

- Whether through a website or a virtual newsletter, most defendants utilize the internet to some extent

Provides video content

- Doesn't have to be the "main" business – incidental video use may be enough

Use of Cookies

- Primarily applicable to third-party cookies – Issue is the provision of PII *to* the third party

Subscriber or account creation

- Represents an ongoing relationship with consumers

FIGURE 1

Evidence included in complaint
General Mills

Evidence included in complaint
Star Tribune Media Company

Exemplary Cases

Motions to Dismiss ***Granted***

- ***Keith Carroll v. General Mills, Inc.*, No. 2:23-cv-01746, ECF No. 36 (C.D. Cal., Sept. 1, 2023)**
  - General Mills was not a "video tape service provider"
  - Plaintiff also not a "consumer" of audio-visual goods from General Mills

- ***Brown v. Learfield Communications, LLC,* No. 1:23-CV-00374, (W.D. Tex. Jan. 29, 2024)**
  - Plaintiff did not qualify as a "consumer" (specifically, not a "subscriber") due to a lack of an ongoing relationship

- ***Ellis v. The Cartoon Network, Inc.*, Case No. 1:14-cv-00484-TWT, ECF No. 35 (N.D.Ga, Oct. 8, 2014)**
  - Android ID and viewing history were not considered "personally identifiable information" (though Plaintiff was found to be a "subscriber" and therefore a "consumer")

- ***Martin v. Meredith Corp.*, Case No. 1:22-cv-04776-DLC, ECF No. 57 (S.D.N.Y., Feb. 17, 2023)**
  - While PII was disclosed, cookies did not disclose whether person had "requested or obtained specific video materials or services"

Exemplary Cases

Motions to Dismiss ***Denied***

- ***Lebakken v. WebMD, LLC*, 640 F. Supp. 3d 1335 (N.D. Ga. 2022)**
  - Motion to dismiss was *denied* because the newsletter at issue was considered a "service"
    - Didn't need to specifically receive video content from the Defendant; needed to receive some good/service from a Defendant that also provides video services
- ***Feldman v. Star Tribune Media Company LLC*, Case No. 0:22-cv-01731-ECT-TNL, ECF No. 32 (D.Minn., Mar. 7, 2023)**
  - Argument against "knowledge" requirement was not appropriate for MTD and so was not sufficient to dismiss claim
  - Consent (claimed by Defendant) was also an affirmative defense, not appropriate for MTD
- ***M.K. v. Google LLC*, Case No. 5:21-cv-08465, ECF No. 91 (N.D.Cal., Aug. 1, 2023)**
  - "Ordinary course of business" exception was affirmative defense, not appropriate for MTD
- ***Jancik v. WebMD*, Case No. 1:22-cv-00644-TWT, ECF No. 40 (N.D.Ga, Nov. 4, 2022)**
  - "Knowledge" requirement was at least pled in complaint, though it could be challenged in later stages of litigation

What Works? What Doesn't?

More Successful on MTD
Plaintiff doesn't qualify as a consumer
Whether information shared is considered PII
Whether defendant is a "video tape service provider"
Providing live video, instead of pre-recorded content

Less Successful on MTD
Stating lack of "knowledge" of PII transmission
Plaintiff "consented" to transmission
Transmission was made according to "ordinary practice of business"

Takeaways

- Be upfront about use of cookies (especially third-party cookies) and provide users the ability to provide / withdraw their consent
  - 18 U.S.C. § 2710(b)(2) provides exceptions for when PII can be disclosed to "any person" with "informed, written consent … of the consumer"
  - The issue in any VPPA claim is providing information to some third-party without user consent
- VPPA Actions are an attractive target for class actions because they provide $2,500 recovery and potential attorneys' fees
  - Claims are also quite broad, with definition of "video tape service provider" appearing to be a fact-intensive inquiry
  - Evaluate arbitration provisions and class action waiver provisions in subscriber agreements, or in other terms under which users access video content
- Crystalize business offerings, where possible, to differentiate from being a "video tape service provider"
  - Can support argument for early dismissal of any actions
- Note that VPPA requires separate and distinct consent, and website operators may not be able to rely on privacy policies alone

THE ROLE OF COOKIES 02

ECPA AND OTHER LAWS

BAKER BOTTS

What Are Cookies?

- Small pieces of code which store information about the user to enable some additional functionality/feature
  - Can store login information or preferences
  - Can track browsing history and other information related to the user's habits

- First-party v. Third-party
  - First-party cookies are created and stored by the website you are visiting directly. They are used to collect user data for analytics, remember settings, store login information
  - Third-party cookies (e.g. Google AdSense/Facebook Pixel) are created and placed by third parties other than the website you are visiting directly.

- Customizable – Even third-party cookies can be configured differently
  - *Specific* use is what creates the risk

- Since they inherently track a user's behavior, and in some cases, communications, they can implicate various privacy laws

Implications

Why cookies?
• Improve usability of sites   • Sometime necessary for functioning • Found in some form on *most* websites • Used to monetize sites – either directly or indirectly

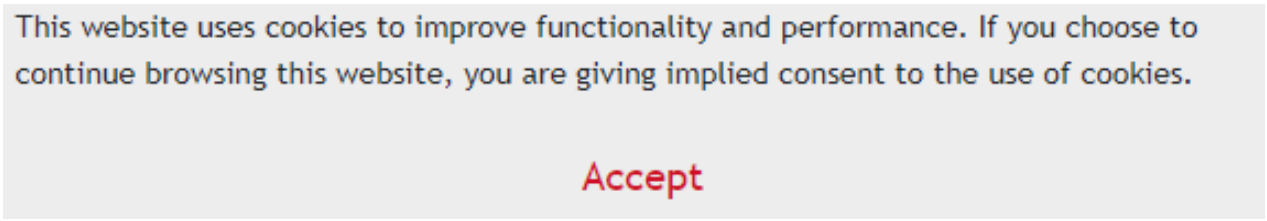
What information
• User's names • Browsing history • Device information • Preferences • Account names and passwords

Applicable laws
VPPA
Electronic Communications Privacy Act (ECPA)
EU Cookie Directive
State-specific variants (CPRA, Tex. DPSA)

How to Handle Cookies?

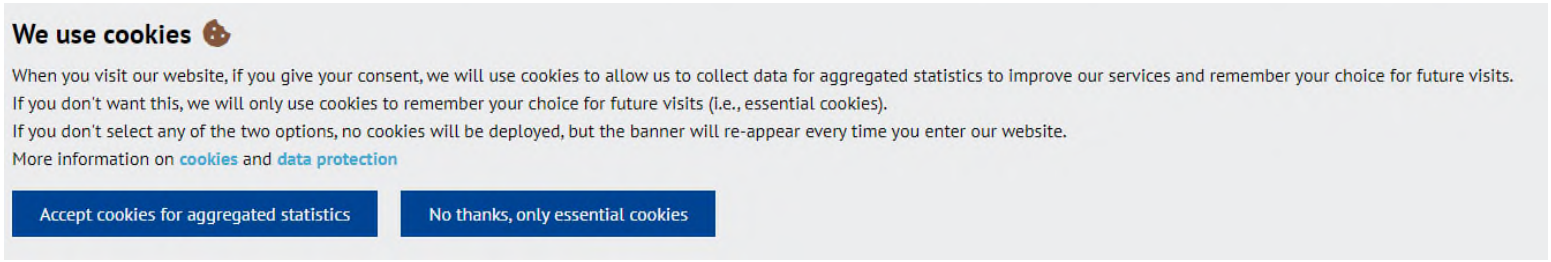
Cookie Banners?

Provide basic information on cookies



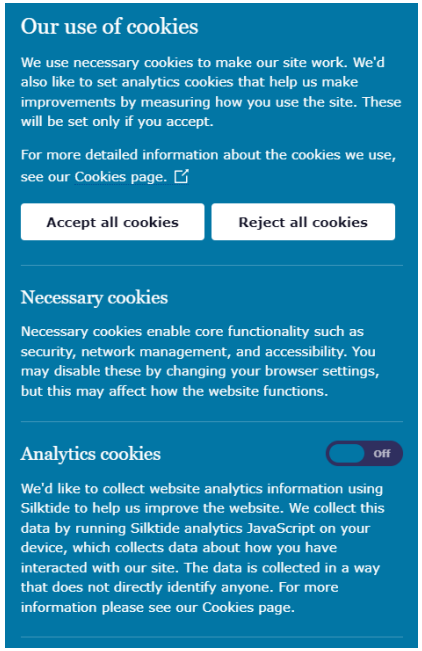
Cookie banner on Baker Botts' U.S. website

Provide options but limited information



Cookie banner on European Data Protection Board website

Provide options and specific information about cookies being used



Cookie banner on UK's Information Commissioner Office website

Necessity?

- Not all jurisdictions require cookie notice
- Use of cookies might not necessitate notice

Statutes which Implicate Cookies

ECPA 18 USC §2511
Prohibition against:
1) Intentional
2) interception of
3) **the contents** of
4) an electronic communication
4) using a device
Except where:
interceptor is a party to the communication

State Variants

California Invasion of Privacy Act of 1967

- Requires *two party* consent to record conversations (including telephone conversations)

Pennsylvania Wiretapping and Electronic Surveillance Control Act

- Allows for a private right of action
- If one party intercepts any wire, electronic or oral communication without consent from both parties, then they are guilty of a felony

Texas Penal Code § 16.02

- Creates *criminal* penalties for unauthorized interception of communications

ECPA Cases

Primary Claim: Tracking cookies (undisclosed to the user) intercept information about a user's internet browsing/traffic history

- ***In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015)**
  - Class asserted violation of ECPA through Google's use of cookies on user's browsers – Multi-district litigation consolidated into the District of Delaware
  - Alleged violation of Section 2511 of the ECPA and Section 2701 of the Stored Communications Act based upon Defendants' use of cookies for advertisements
  - **Dismissed ECPA claims – Defendants were a proper *party* of the relevant communication, so did not improperly use cookies**
  - **Dismissed SCA claims – No "facility" implicated** – Personal Computer does not comprise a "facility" under the Act
- ***In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020)**
  - Class action asserted violation of ECPA, CIPA, SCA, and other state law claims
  - **"Simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception"**
    - "[E]ntities that surreptitiously duplicate transmissions between two parties are not parties to communications within the meaning of the Act."
  - Determined that bulk collection of user's browsing history (regardless of any consideration of sensitivity of history) plausibly pled harm (or risk of harm) to convey standing

Other Cases Dealing with Cookies

- ***Roland v. Chive Media Group, LLC*, Case No. 1:23-cv-00389 (W.D. Tex. 2023)**
  - Proposed class action against Chive Media for it's use of Facebook Pixel
  - Claims primarily brought under the VPPA
  - Transferred to N.D. Ill. and settled shortly after

- ***Brown v. Google*, Case No. 4:20-cv-03664 (N.D. Cal. 2020)**
  - Proposed class action seeking $5 billion in damages over Google's use of cookies
  - Brought under the Electronic Communication Privacy Act and other state laws
  - Currently working on settlement agreement of undisclosed amount

- ***John Doe v. Cedars-Sinai Health System,* Case No. 2:23-cv-00870 (C.D. Cal. 2023)**
  - Claims that cookies used by medical center transmitted patients' habits to AdTech companies (e.g. Google Ads)
  - Brought under various state statutes, including common-law invasion of privacy
  - Remanded to state court to adjudicate state law claims

Takeaways

- ***Cookies*** by their nature are usually unnoticed (if not unknown) by users
  - If these cookies are tracking user behavior and visits, it implicates privacy concerns
  - They provide a new avenue for various privacy claims to be brought against an almost ubiquitous internet behavior

- Companies should determine ***whether*** and ***how*** cookies are utilized in business strategy, including:
  - To what degree you need cookies for your business?
  - How are you providing notice to consumers?
  - Are your cookies first-party or third-party?
  - Are you obtaining consents?

- But browsing history isn't the only private information that can be collected. What about even more personal information?

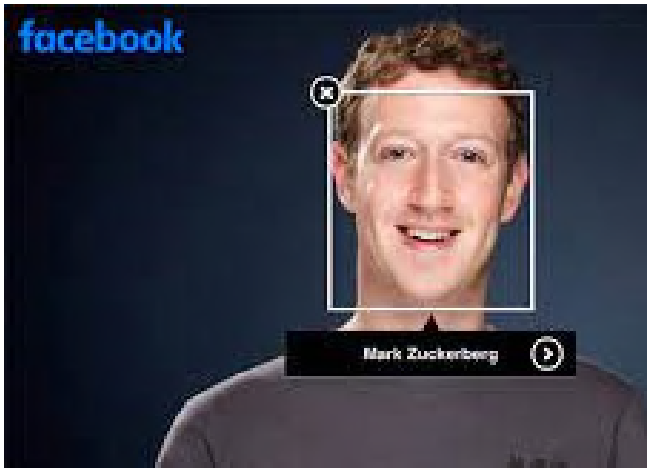
BIOMETRICS 03

BIPA AND OTHERS

BAKER BOTTS

What Are Biometrics?

- Coverage will depend on the state-specific law, but it generally refers to a physical feature that uniquely identifies you



- Generally, will include things like:
  - Face scans
  - Voice recognition
  - Fingerprints
  - Retina images

- Several states have Biometric laws:
  - Texas - CUBI
  - Illinois - BIPA
  - Washington – My Health My Data Act

Texas Capture or Use of Biometric Identifiers

11 Tex. Bus. & Comm. Code § 503.001

Applies to
Retina/Iris Scan Fingerprint Voiceprint "record of hand or face geometry"

Requires
Commercial Purpose & Notice (before capture) & Consent

Other Elements
$25,000 fine per violation **No** private right of action Must use reasonable security measures to protect

Washington My Health My Data Act

19 RCW § 19.375

Applies to

Any data generated by automatic measurements of an individual's biological characteristics

Requires

Commercial Purpose
&
Notice (before capture) **OR** consent **OR** mechanism to opt-out of subsequent use

Other Elements

No private right of action

Must use reasonable security measures to protect

Illinois Biometric Information Privacy Act

2008

BIPA passed
- Directed to biometric identifiers
- Requires public, written policies related to any collection
- Requires permission to collect biometrics
- **Allows for a *private right of action***

Cothron v. White Castle Sys. (2023)

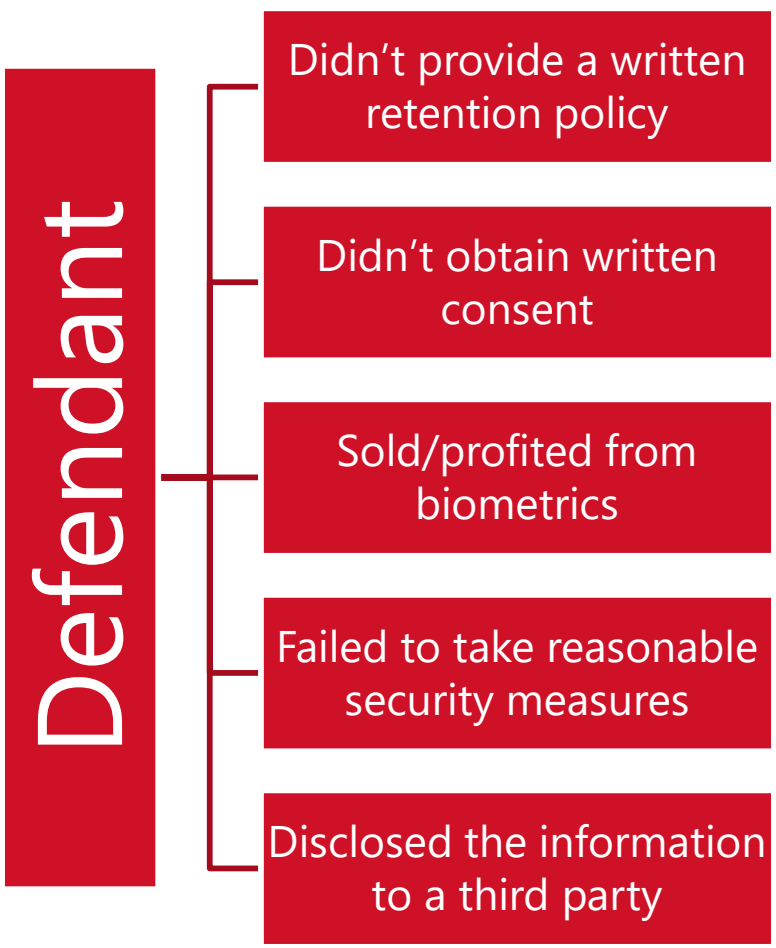
Illinois Supreme Court holds that BIPA claims accrue for *each* collection and dissemination of biometric information
- Not only first time
- Certified question from Seventh Circuit Court of Appeals

Tims v. Black Horse Carriers, Inc. (2023)

Illinois Supreme Court holds that *five-year* statute of limitations applied to BIPA claims
- Rejected one-year limit based on other privacy violations

Fingerprint of a BIPA Claim

Several potential provisions, and plaintiffs often bring claims under multiple provisions



Different than just a privacy policy or even obtaining consent of the party

No explicit notification requirement in BIPA, but now data breach may bring additional risk

Exemplary Cases

Primary Claim: Recognition technology used without notice/consent

- ***Hogan v. Amazon.com, Inc.*, Case. No. 21-C-3169 (E.D. Ill. 2021)**
  - Class action against Amazon's Photo service which performed face recognition without appropriately informing subscribers (consumer case)
  - August 2023 – Court dismissed one of two claims in Amended Complaint
    - Found that complaint did not properly allege that Amazon "failed to comply with its own policy" regarding deletion of stored information
  - Trial currently set for December 2024

- ***Hoskin v. Pepsico, Inc.*, Case No. 7:23-cv-06413 (S.D.N.Y. 2023)**
  - Extraterritorial application of BIPA
  - Accuses PepsiCo of creating a "voiceprint" of certain employees in distribution centers (employer / employee case)
    - Headset which provides instructions *and* matches responder's voice against an (allegedly) pre-stored print

- ***In re Facebook Biometric Information Privacy Litigation*, 522 F. Supp. 3d 617 (N.D. Cal. 2021)**
  - Accused Facebook's "tagging" features of stored facial recognition scans without notice and consent
  - Approved $650 million settlement based on BIPA claims (other big settlements: $100M (Google); $35M (Snapchat))

Takeaways

- Distinction between image ***collection*** and image ***recognition***
  - BIPA explicitly excludes photographs and general descriptions about the person
  - The use of images is what matters – facial recognition, authentication or verification are the types of "biometrics" that implicate BIPA

- Collection is not inherently a problem
  - When you start using that information to verify a consumer, or a worker, or anyone, then BIPA comes into play

- Significant damages are available:
  - Caselaw allows for repeated violations that can easily add up, especially since damages can be dated back 5 years
  - *See Cothron v. White Castle Systems Inc.* (Illinois Supreme Court)

- **How can you use biometrics?**
  - Receive ***written consent*** before you begin a new biometrics activity
  - De-identify – This inherently makes the information non-biometric
  - Be transparent – use robust privacy policy that authorizes use and retention of biometric information

TEXAS DATA PRIVACY 04

TEXAS DATA PRIVACY AND SECURITY ACT (2023)

BAKER BOTTS

Texas Data Privacy and Security Act (TDPSA)

Logistics

• Effective July 1, 2024
• No-private right of action
  • $7,500 fine per violation
  • 30-day cure period

Scope
• Conduct business in Texas OR service used by Texas residents; • Process OR sell personal data; AND • Not a small business

Key obligations (for Controllers)	
Minimize data collected	Provide privacy notice
Establish 2+ secure methods to allow consumers to communicate with controller	Ensure *vendors* implement/maintain sufficient security measures
Reply to requests from consumers within **45 days**	Disclose sale of data for advertising purposes
Obtain specific consent for processing "sensitive" personal data	In some situations, perform Data Protection Impact Assessments

Samir A. Bhavsar

Partner | Dallas

+1.214.953.6581

samir.bhavsar@bakerbotts.com

EDUCATION/HONORS

J.D., University of Michigan Law School, 1996

B.S., Electrical Engineering, University of Michigan, 1994

Samir Bhavsar is a technically agile, full-service intellectual property lawyer who works closely with his clients who praise him for being "quick to understand the facts" and comment that the "quality of his work is excellent, is done efficiently and he provides a very well written product." *The Legal 500* (2010). They also value his combination of skills, noting that Mr. Bhavsar "knows his patent prosecution, licensing and litigation - this many skills in one person is rare." *The Legal 500* (2013). As a former Chief IP Counsel, Samir "understands the client mentality better than most and applies his considerable faculties in driving quality prosecution, litigation, and licensing outcomes." *IAM Patent 1000* (2021). Samir's practice also extends to data privacy, including strategic guidance and counseling. He is certified as an Information Privacy Professional for the U.S. (CIPP/US) and Europe (CIPP/E) by the International Association of Privacy Professionals.

Clients find Samir's prior experience as a Chief IP Counsel key to assisting them with developing valuable patent portfolios through strategic patent mining, preparation and prosecution. He has twice been recognized as a "Leading Lawyer" by *The Legal 500* (2010 & 2013) for his work in this field. Clients also rely on him to draft and negotiate complex patent, software, and other agreements directed to inbound and outbound licensing and the ownership of technology assets. Samir performs IP due diligence and freedom-to-operate studies and offers advice regarding intellectual property issues that arise in initial public offerings, mergers, acquisitions, credit facilities and other corporate transactions.

Clients find Samir's technology experience to be extensive and diverse. In the last ten years alone, he has worked on a wide range of cutting-edge technologies, including: Artificial Intelligence (AI) and machine learning; Robotics, drones, and autonomous vehicles; Augmented and Virtual Reality (AR/VR); Computer vision and image processing; Cybersecurity; IoT; smart homes and devices; Heating, ventilation, and air conditioning (HVAC); FinTech; Telecommunications and Internet-enabling technologies; Cloud and edge computing; Big data analytics; Blockchain; Biotechnology and medical devices; Electronic gaming; Contactless e-commerce and delivery; Semiconductor devices and manufacturing.

Samir has served on many Boards and Steering Committees for diversity organizations locally and nationwide, including the Dallas Bar Association, NAPABA and the Texas Minority Counsel Program. He enjoys mentoring young lawyers both within and outside the firm. Samir is a graduate of the Dallas Regional Chamber's 2019 Leadership Dallas class.

Nick Palmieri

Associate | New York

+1.212.408.2640

nick.palmieri@bakerbotts.com

EDUCATION/HONORS

J.D., Indiana University Maurer School of Law, 2019

B.S., Physics, Rensselaer Polytechnic Institute, 2015

Nick Palmieri serves in the Intellectual Property Practice of the firm's New York office. He has experience with a wide range of intellectual property matters, including patent prosecution and litigation, which span a wide range of technological fields, including medical devices, electrochemical devices, and many other emerging areas. In addition, Mr. Palmieri has experience in the data privacy space, having assisted clients with data breach notification requirements and compliance with GDPR and CCPA regulations. He is certified as an Information Privacy Professional for the U.S. (CIPP/US) by the International Association of Privacy Professionals.

In addition to his client work, Mr. Palmieri has written about a number of topics, including data privacy law, as well as developing trends related to the regulation of artificial intelligence. Mr. Palmieri's works span a number of publishers, including the *CPI Antitrust Chronicle*, *The Journal of Robotics*, *Artificial Intelligence & Law*, *Financier Worldwide Magazine*, *The Indiana Law Journal*, *The Willamette Journal of International Law and Dispute Resolution*, and *The Hastings Science and Technology Law Journal*.

AUSTIN

BRUSSELS

DALLAS

DUBAI

HOUSTON

LONDON

NEW YORK

PALO ALTO

RIYADH

SAN FRANCISCO

SINGAPORE

WASHINGTON

bakerbotts.com