Buchanan

New Frontiers In Privacy Enforcement and Litigation

September 13, 2023

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Speakers

Jonathan D. Janow
Shareholder | Litigation
Phone: 202 452 6057
Email: jonathan.janow@bipc.com

Rebecca N. Knight
Principal Corporate Counsel, Privacy
Cisco
Email: rebknigh@cisco.com

Jennifer M. Oliver
Counsel | Litigation
Phone: 619 685 1990
Email: jennifer.oliver@bipc.com

Agenda

1. Relevant Laws
    - FTC Act
    - CPPA
    - Federal wiretapping laws
    - State wiretapping laws
    - VPPA
    - State privacy laws (CCPA, WA MHMDA)
    - Common law claims
2. Practices and Technologies Giving Rise to Enforcement
3. Overview of Agency and Private Plaintiff Enforcement
4. Defenses
5. Risk Assessment, Mitigation, Strategy, Resolution

Relevant Laws

The FTC Act

- Broad consumer protection act used to enforce consumer privacy rights
- Used to prevent unfair competition, seek monetary redress for consumers
- No private right of action, used only by the FTC
- Typically allege unfairness, failure to disclosure, and/or misrepresentations in violation of 15 U.S.C. section 45

CCPA

- California Consumer Privacy Act of 2018 (as amended by the CPRA in 2020)
- Gives consumers the right to know, to delete, to opt-out, to non-discrimination, to correct, and to limit the use and disclosure of sensitive personal information
- CPPA enforces most sections of the law
- Private right of action for data breaches with statutory damages of up to $750 per
- If using Pixels or other technology to target Google or social media ads is sharing personal information, then CCPA rights may be implicated

Federal Wiretap Act

- Private right of action used by private plaintiffs in court (mostly class actions) and arbitration (class and individual actions)
- 18 U.S.C. § 2511 et seq
- Also known as the Omnibus Crime Control and Safe Streets Act of 1968 or the Electronic Communications Privacy Act of 1986 (amended the 1968 version)
- Prohibits knowingly intercepting or procuring another to intercept communications
- Statutory damages of $10,000 or $100 per day for each violation

California Invasion of Privacy Act (CIPA)

- Private right of action used by private plaintiffs in court (mostly class actions) and arbitration (class and individual actions)
- California Penal Code Sections 631, 632, 632.7, 637
- 50-year-old statute given a new lease on life
- Statutory damages of $5,000 for each violation or up to $10,000 per violation for previous offenders

Cal. Pen. Code 637.2(a)(1)

Similar State Laws

- FSCA: Florida Security of Communications Act
  - Florida Statutes Section 934.03
- WESCA: Pennsylvania Wiretapping and Electronic Surveillance Control Act
  - 8 Pa. C.S. § 5701 et. seq.
- California Unauthorized Access to Computer Data Act (CUACDA)

VPPA

- Video Privacy Protection Act of 1988 (federal)
- 18 USC § 2710 et. seq.
- Creates potential liability for any **video tape service provider** who **knowingly discloses**, to any person, **personally identifiable information** concerning any consumer of such provider shall be liable to the aggrieved person
- Protects “generally a consumer's substantive privacy interest in his or her video-viewing history”
- Statutory damages of up to $2,500 per violation, also punitive damages and attorneys' fees

Other Claims

- Invasion of privacy (generally and under state constitutions)
- Unjust enrichment
- Breach of confidence (where duty of confidence exists)
- Injunctive and declaratory relief

Practices and Technologies Giving Rise to Enforcement

Meta Pixel

- Code, courtesy of Meta, that can allow website owner to understand consumer browsing patterns and actions
- Can be used to target advertising and measure the results of ads
- When Facebook users enable cookies and allow Facebook to collect certain data, it can share those users' activities/sites by running the Pixel through their Facebook user id

Session Replay Software

- Commonplace web optimization software
- Code helps site owners understand and improve the user experience
  - Points of error, frustration or confusion
- Usually, "[e]verything is encrypted at the client device and exposed personal information is never sent across the network…." which is why "multiple top five banks, insurance, and telecom companies" also trust this technology
- Plaintiffs allege software is active from outset of browsing session
- Can also capture viewership of on demand video content

"What is Session Replay?" https://www.quantummetric.com/product-analytics/session-replay/.

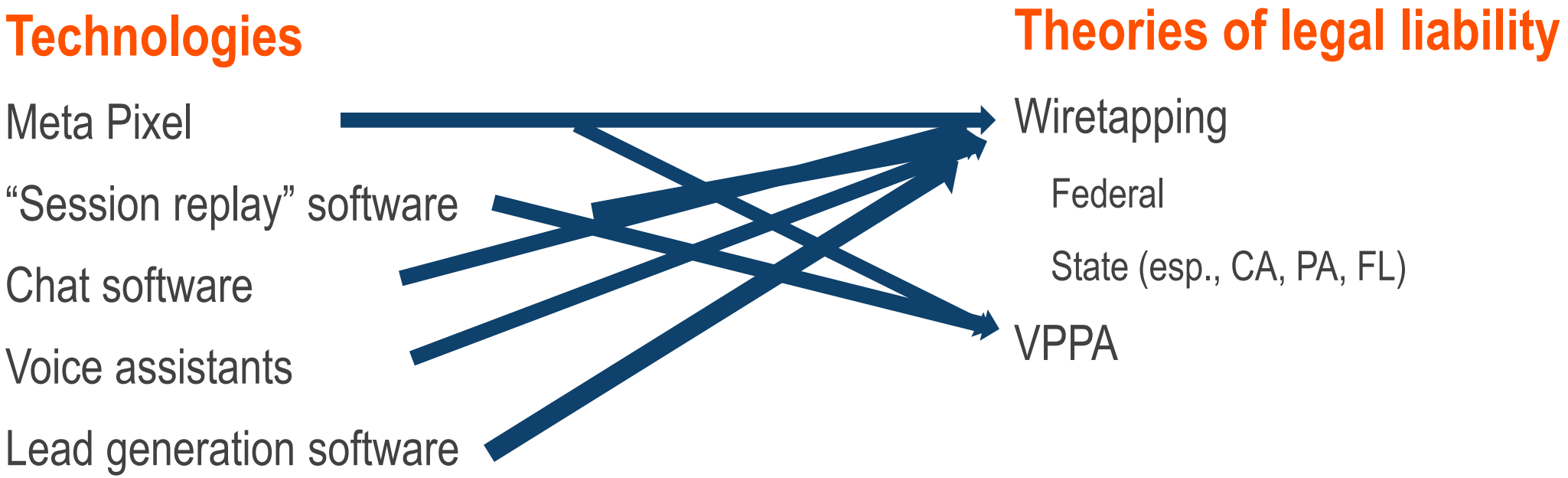
Chat

- Commonly used manned or automated feature on consumer facing websites
- Often used for customer service purposes in place of a phone call
- Can also be used to boost sales
- Often facilitated by third party software

Lead Generation Software

- Leadlander, Leadfeeder, etc.
- Software compiles reports of name, copay name, IP address, and which pages were visited and for how long
- Complaints suggest this “doxes” site visitors without their consent and allows the software vendors to use the data for other purposes

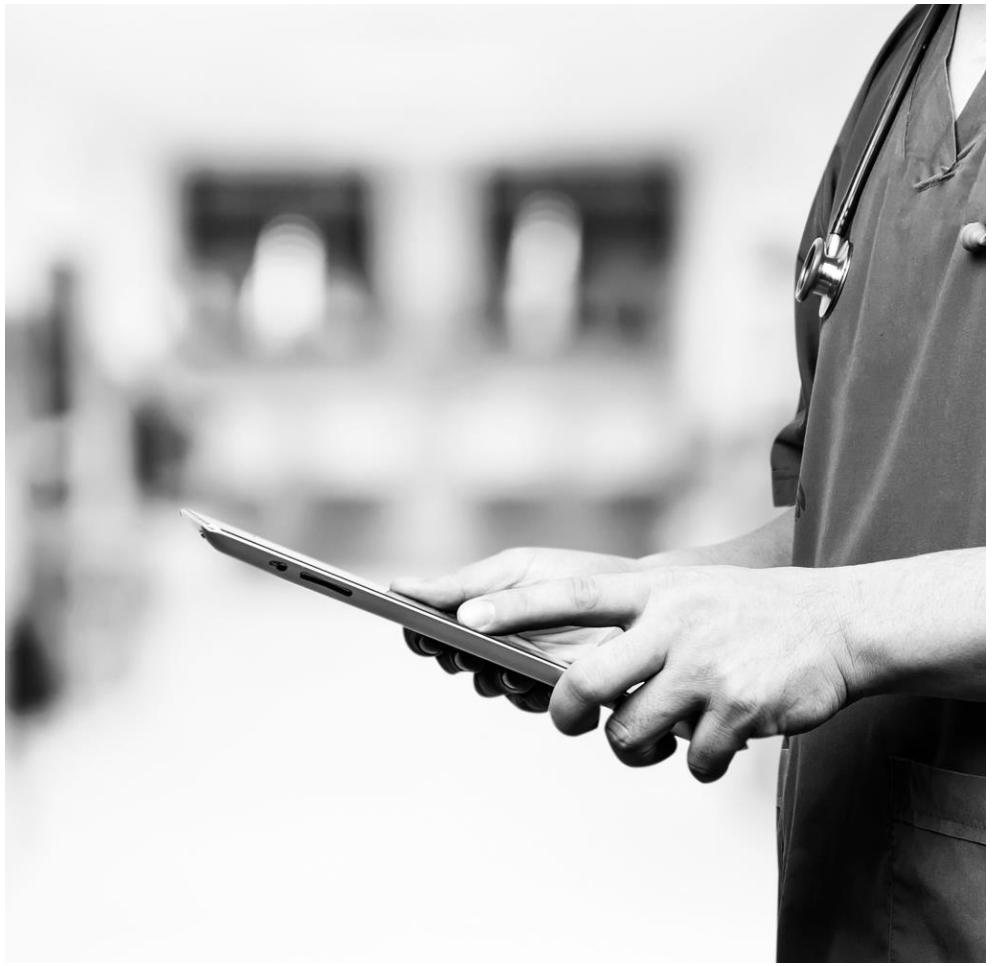
Technologies and Theories



Overview of Agency and Private Plaintiff Enforcement

FTC Enforcement Actions

- Enforce the unfair competition provisions of the FTC Act
- Especially focused on healthcare data lately
- In July 2023, the FTC and DOH sent a joint letter to 30 hospital systems and telehealth providers to alert them about the risks and concerns associated with technologies such as the Meta Pixel and Google analytics that can track online activities



Examples of FTC Enforcement Actions

- In the matter of BetterHelp
  - FTC alleged that the company used and disclosed email addresses, IP addresses, and health information to Facebook, Snapchat, Criteo, and Pinterest for advertising purposes despite claiming it would only disclose health data for limited purposes.
  - Consent order:
    - BetterHelp agreed to pay $7.8 million to provide partial refunds to the consumers.
    - Banned BetterHelp from sharing consumers' personal information for re-targeting.
    - Must obtain affirmative express consent before disclosing personal information to certain third parties for any purpose; put in place a comprehensive privacy program that includes strong safeguards to protect consumer data; direct third parties to delete the consumer health and other personal data that BetterHelp shared; and limit how long it can retain personal and health information according to a data retention schedule.

Examples of FTC Enforcement Actions (Cont.)

- United States v. GoodRx
  - USAG sued for violation of FTC act and Health Breach Notification Rule for alleged
    - disclosure of health and personal information to third parties (Facebook, Google Etc.)
    - failure to limit third-party use of health information
    - misrepresentation of compliance with the Digital Advertising Alliance principles
    - misrepresentation that consumer's health information was protected under the Health Insurance Portability and Accountability Act ("HIPAA")
    - failure to implement sufficient policies or procedures to prevent the improper or unauthorized disclosure of health information, or to notify users of breaches of that information, and
    - failure to provide notice and obtain consent before the use and disclosure of health information for advertising.

Examples of FTC Enforcement Actions (Cont.)

- United States v. GoodRx
  - GoodRx must pay a $1.5 million civil penalty for violating the rule and is subject to an order that:
    - Permanently prohibits the sharing of health data for ad
    - Requires users affirmative and express consent for any other sharing
    - Requires the company to seek third party deletion of data
    - Limit retention of data according to a publicly posted schedule, including justification for collecting the data
    - Implement a mandated privacy program that includes strong safeguards to protect consumer data

Enforcers

Attorney General (OAG)

- Chief enforcer of all laws
- Civil enforcement, in-court
- Investigations under 11180
- No more notice/cure
- No more CCPA rulemaking

Agency (CPPA)

- CPRA/CCPA
- Administrative
- 1789.199.65 + Auditor
- Discretion to cure
- Rulemaking authority
- Subject to Bagley-Keene Act

Enforcement Priorities

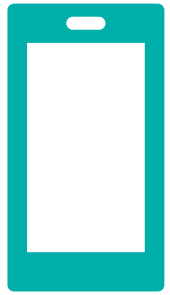
Attorney General

- TBD

Agency

- Privacy notices and policies
- Right to delete
- Implementation of consumer requests

Investigative Sweeps



2023

Large employers

Connected cars

Popular mobile apps

2022

Online retailers

Loyalty programs

Enforcement Action

- Sephora – the first and only public enforcement action under the CCPA to date.
  - Issues:
    - Failure to disclose sale of personal data to consumers and
    - Failure to process opt-out requests
  - Resolution:
    - Pay $1.2 million
    - Inform consumers that it sells their personal data, and
    - Honor consumers' requests to opt out of such sales

Key Takeaways

Pay close attention to investigation trends and (shifting) priorities.

Mark Data Privacy Day (January 28th) on your calendar.

Session Replay/Lead Generation Cases

- Allege that companies utilizing session replay software to track user behavior on a website violate wiretapping laws if no consent
- Some allege the session replay vendor is the wiretapper, some allege the company is the wiretapper
- Some allege federal wiretap claims
- Many allege state wiretapping law violations (e.g., CIPA)
- May also allege violation of VPPA where data regarding viewing of video content is captured
- Some allege common law claims

Session Replay/Lead Generation Litigation

- Florida courts say have ruled software is “definitionally excluded” from federal and state wiretap statutes because it is not a wiretapping software; rather, it is a “software which tracks a website browser’s movements.”
- Other states have yet to rule definitively at the supreme court/appellate level
- CA courts are dismissing many cases with leave to amend, allowing some to proceed, especially if third party use of data for own purposes is alleged
- Third Circuit has reinstated dismissed claims

Chat Cases

- Allege that consumer websites with a “chat” function (usually for customer service) can violate wiretapping laws absent consent from the consumer
- Probably weaker than session replay cases because consumer knows they are “communicating” with website owner
- Plaintiffs may allege aiding and abetting interception by a third-party chat function provider
- Potential claims under federal or state wiretapping acts
- Some allege common law invasion of privacy claims as recognized state by state

Meta Pixel Cases

- Allege that use of the Pixel tool violates wiretapping laws or VPPA absent explicit consent
- Easy for consumers to see which sites are collecting data through the Pixel in their own Facebook settings
- Many cases focused on healthcare providers or other defendants where consumers may search for or view more “personal” or “private” content
- Allege violation of wiretapping laws
- May also allege violation of VPPA where video content is provided

Defenses

Defenses to Wiretapping Claims

- Lack of intent
- Explicit consent or authorization
  - Opt-in consent to terms and conditions/privacy policy
  - Membership in loyalty programs
  - Checking a box to make a purchase
  - Implied consent may not be enough (see mitigation measures supra)
- Party exemption
  - Cannot eavesdrop on your own conversation
  - “Only a third party can listen secretly to a private conversation.”
  - *But* can allege third party aiding and abetting, i.e., that the session replay vendor is the interceptor and website owner facilitated

Defenses to Wiretapping Claims (Cont.)

- Vendor as an "extension" of website owner
  - *Graham v. Noom*, Inc., 533 F. Supp. 823, 829 (N.D. Cal. 2021), plaintiff alleged that use of session replay software violated CIPA
  - Court found no plausible allegations of wiretapping under California law because consumer and defendant were the only parties to the "communication"
  - Even if third-party session replay software vendor was the alleged interceptor no liability because that vendor operates as an "extension" of the Defendant by providing "a tool — like [a] tape recorder…— that allows [Defendant] to record and analyze its own data in aid of [Defendant's] business"
  - *See also Johnson v. Blue Nile, Inc.*, No. 20-cv-08183-LB, 2021 BL 306751 (N.D. Cal. Aug. 13, 2021)

VPPA Defenses

- Standing
- Plaintiff not a consumer ("any renter, purchaser, or subscriber of goods or services from a video tape service provider")
- Defendant not a "video tape service provider"
- No "disclosure:" it is the consumer's web browser, as opposed to the company website, that transmits the purportedly identifying consumer data
- Defendant did not "knowingly" disclose because no access to or knowledge of the cookie on the web browser
- VPPA is unconstitutional because it restricts commercial speech in violation of the First Amendment

Standing Defenses

- Article III standing
  - Generally only applies in federal court
  - U.S. Supreme Court has held that a plaintiff must establish “standing” to bring a lawsuit in federal court
  - The suit must be based on an actual or imminent alleged injury that is concrete and particularized
  - Circuit split on Article III Standing in privacy cases
  - Consider: do you want to end up back in state court?
  - Plaintiffs are filing in state court, forcing defendant to remove; defendant cannot avail itself of federal jurisdiction and then disavow it
  - Tester plaintiffs generally acceptable

Jurisdictional Defenses

- Personal jurisdiction
  - Plaintiff must allege Defendant (1) committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in the forum state
  - E.g., claims by a California class against an out of state defendant
  - Consider: plaintiff may refile in Defendant's home state, leaving a court unfamiliar with state statutes to interpret them

Risk assessment, Mitigation, Strategy, Resolution

Risk Assessment

- Valuation
  - Per-violation statutory damages for thousands of visitors, some who have visited multiple times
  - Plaintiffs try to stack multiple claims for a single visit
  - Shorter statute of limitations for most claims (CIPA = one year, WESCA, VPPA and federal wiretapping = two years)
  - Pixel classes limited to Facebook users with certain settings

Risk Assessment (Cont.)

- Higher Risk Sectors
  - Healthcare providers and hospital systems
    - One complaint claims 664 have sent data using Pixel
    - *In Re Meta Pixel Healthcare Litigation* MDL pending
    - Consider HIPAA and *Dobbs*
  - Universities and athletic associations
  - Consumer facing e-commerce websites, especially retail
  - Media outlets
  - Consumer facing web pages containing on demand video content

Risk Assessment (Cont.)

- Class Certification/Rule 23 Considerations
  - Often see state sub-classes (for state laws) and nationwide classes (federal laws)
  - Ascertainability and notice
  - Class definition
  - Uninjured class members
- Other Risks
  - Regulatory enforcement actions
  - Data breach reporting laws

Mitigation

- Mandatory Arbitration Clauses and Class Action Waivers
  - May help prevent filings in court/class action approach
  - Plaintiffs are also skilled at mass arbitrations, which can be costly, equally bad PR, and lead to inconsistent results
  - Clauses must be carefully drafted
    - Consider AAA and other neutrals' consumer due process policies and registration requirements
- Consents and pop ups
  - Consents easier to put in place for chat and video content than session replay
  - Explicit opt-in preferable to notice only
  - Opt-in at outset of browsing session for session replay; consider pausing software until consent is provided
  - Balancing user experience with caution
- Ceasing use of chat, session replay, video content, or Pixel mitigates risk but has obvious drawbacks

Strategy

- Consider pre-suit individual settlement after demand letter?
- Remove to federal court?
- Compel arbitration?
- Raise standing arguments?
- Leverage trade associations to file amicus briefs?
- Append lists of cases filed by certain tester plaintiffs?

Settlement

- Many cases voluntarily dismissed
- Settlement terms not generally available (consider local rules regarding voluntary dismissal of class cases, e.g., in CA)
- Often depends on size of defendant, nature of data, size of potential class
- Most settlements are individual – do not eliminate risk of additional filings
- Classwide settlement difficult (may be easier in Pixel cases)
- One group of healthcare providers paid $18 million for use of cookies, pixels, third party website analytics tools, and associated technologies

Questions? Thank you!

Jonathan D. Janow
Shareholder | Litigation
Phone: 202 452 6057
Email: jonathan.janow@bipc.com

Rebecca N. Knight
Principal Corporate Counsel, Privacy
Cisco
Email: rebknigh@cisco.com

Jennifer M. Oliver
Counsel | Litigation
Phone: 619 685 1990
Email: jennifer.oliver@bipc.com

Appendix