PROGRAM MATERIALS
Program #30202
August 5, 2020

Data Privacy and Cybersecurity Trends and Litigation Developments

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Data Privacy and Cybersecurity Trends and Litigation Developments

HK Data Strategy, Security & Privacy Team | Celesq® and Thomson Reuters / West LegalEdcenter
Wednesday, August 5, 2020

Holland & Knight

Contact

Mark S. Melodia
Holland & Knight LLP
New York, NY
212-513-3583
Mark.Melodia@hklaw.com

Ashley L. Shively
Holland & Knight LLP
San Francisco, CA
415-743-6906
Ashley.Shively@hklaw.com

Anthony J. Palermo
Holland & Knight LLP
Tampa, FL
813-227-6320
Anthony.Palermo@hklaw.com

Agenda

- Evolving societal expectations
- Increasing global regulation
- *First* wave: Data breach
- *Second* wave: Data misuse / over-collection
- *Third* wave: Data ownership / civil rights
- Other issues on the horizon

Evolving Societal Expectations

Holland & Knight

AdTech claims leverage public mistrust for tracking

Digital Ad Fraud Is An Iceberg, There's Much Below The Surface

Dr. Augustine Fou Contributor
CMO Network
I am a digital marketer of 25 years. Now I audit campaigns for fraud.

I Visited 47 Sites. Hundreds of Trackers Followed Me.

By Farhad Manjoo
Graphics by Nadieh Bremer

These Hugely Popular Local News Sites In The US And Canada Are Fake

A network of fake local news sites generated millions of pageviews as part of an ad fraud scheme, researchers say.

Craig Silverman • 7 months ago

Twelve Million Phones, One Dataset, Zero Privacy

One Year Into GDPR, Most Apps Still Harvest Data Without Permission

Facebook Said A Chinese Company Compromised Users With Malware And Then Ran Ads Using Their Accounts

Freaked Out? 3 Steps to Protect Your Phone

Popular VPN And Ad-Blocking Apps Are Secretly Harvesting User Data

Sensor Tower has owned at least 20 apps that track data passing through people's phones.

Craig Silverman • 3 months ago

~~PRIVACY INTERNATIONAL~~

How Apps on Android Share Data with Facebook
(even if you don't have a Facebook account)

Documents show that bail bond companies used a secret phone tracking service to make tens of thousands of location requests.

Sandra Bullock and Ellen DeGeneres Sue Pop-Up Websites Over Misleading Ads

The stars filed a lawsuit on Wednesday as part of an effort to stop fake online endorsements, a growing problem for Hollywood.

By Brooks Barnes and Tiffany Hsu

Popular Apps In Google's Play Store Are Abusing Permissions And Committing Ad Fraud

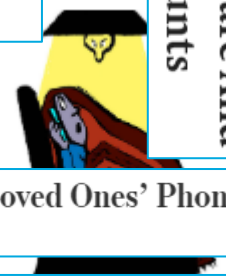
Following a BuzzFeed News investigation, Google removed six apps from the Play store

A Huge Chinese Video App Is Charging People, Draining Their Batteries, And Exposing Data Without Their Knowledge

Why I Put My Dog's Photo on Social Media, but Not My Son's

Unconsenting subjects, data collection and child predators should make any parent pause before posting photos to Instagram and Facebook

By Joanna Stern



You Should Definitely Track Your Loved Ones' Phones. Actually Maybe Not.

How Political Groups Are Harvesting Data From Protesters

Voting and advocacy groups track cellphones of participan
'deeply spooky yet extremely helpful,' says one user

Even Our Lightbulbs Are Spying On Us Now

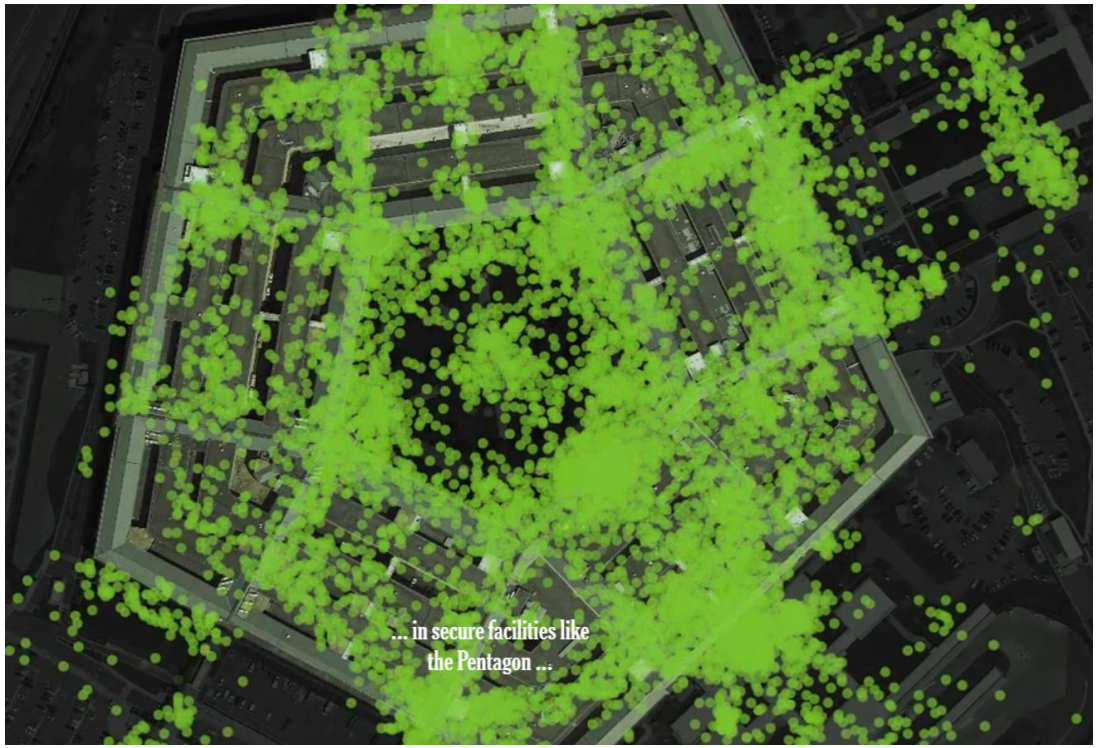
So much for cybersecurity: Identity thieves can use this bright new low-tech idea.

First, the Smartphone Changed. Then, Over a Decade, It Changed Us.

Holland & Knight

Growing awareness of sophisticated digital tracking

- Actual Location of Phones at the Pentagon



Source: [New York Times]

- Data from a single individual's phone over several months

Holland & Knight

Browsers are responding by blocking third party cookies

Apple Safari

- As of March 2020, cross-site tracking cookies now blocked by default
- Safari accounts for **14.4%** of browser usage worldwide

Mozilla Firefox

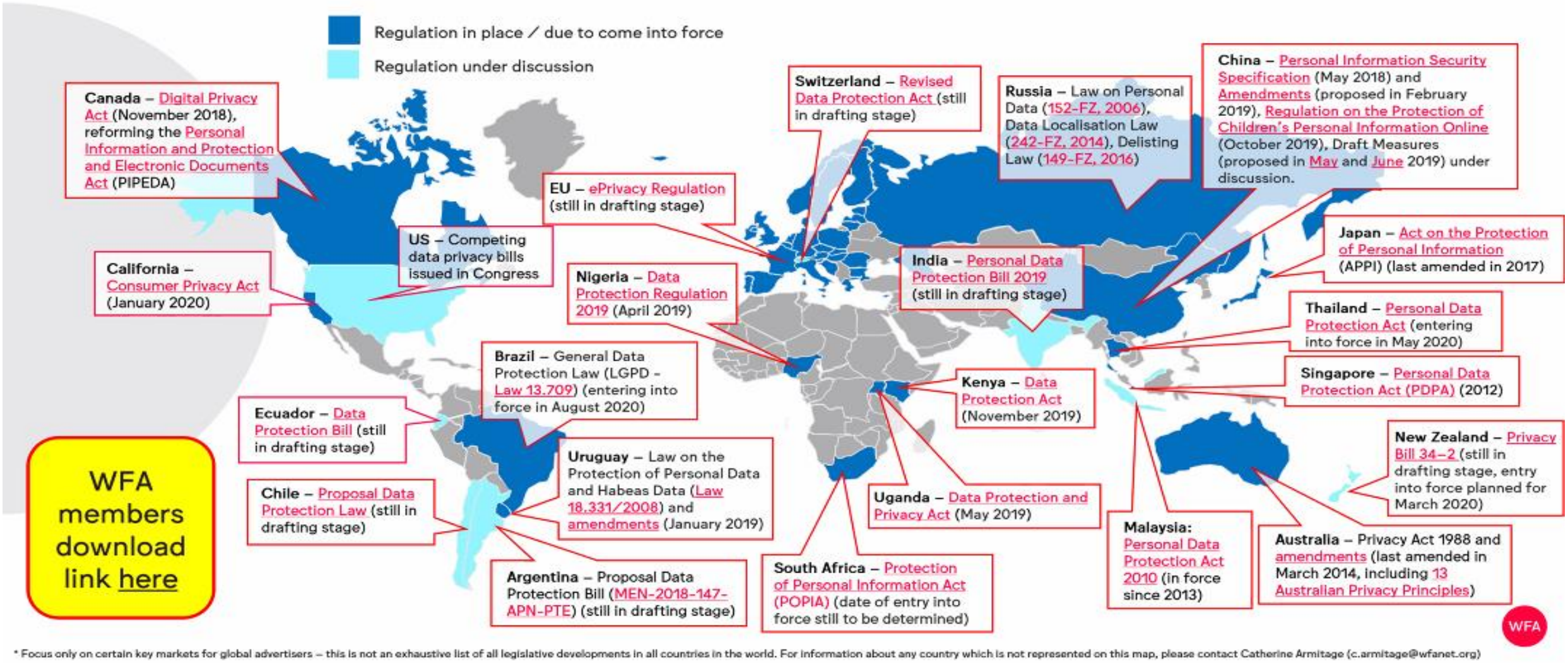
- Beginning June 2019, known trackers blocked by default
- Firefox accounts for **5.1%** of browser usage worldwide

Google Chrome

- Google announced Jan. 2020 that Chrome would phase out third party cookies over next two years
- Chrome accounts for **63%** of browser usage worldwide

Increasing Global Regulation

Regulation: Try to keep up



* Focus only on certain key markets for global advertisers – this is not an exhaustive list of all legislative developments in all countries in the world. For information about any country which is not represented on this map, please contact Catherine Armitage (c.armitage@wfanet.org)

Holland & Knight

Regulation: Rise of the consumer rights

EU General Data Protection Regulation

Consumer rights:

1. The right to **be informed**
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to **restrict processing**
6. The right to data portability
7. The right to **object**
8. Rights in relation to **automated decision making and profiling**.

EU Regulation on Privacy and Electronic Communications ("ePrivacy Regulation")

Simpler rules on cookies: the cookie provision, which has resulted in an overload of consent requests for internet users, will be streamlined. The new rule will be more user-friendly as browser settings will provide for an easy way to accept or refuse tracking cookies and other identifiers. The proposal also clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history) or cookies used by a website to count the number of visitors.

California Consumer Privacy Act (CCPA)

Who is in scope?

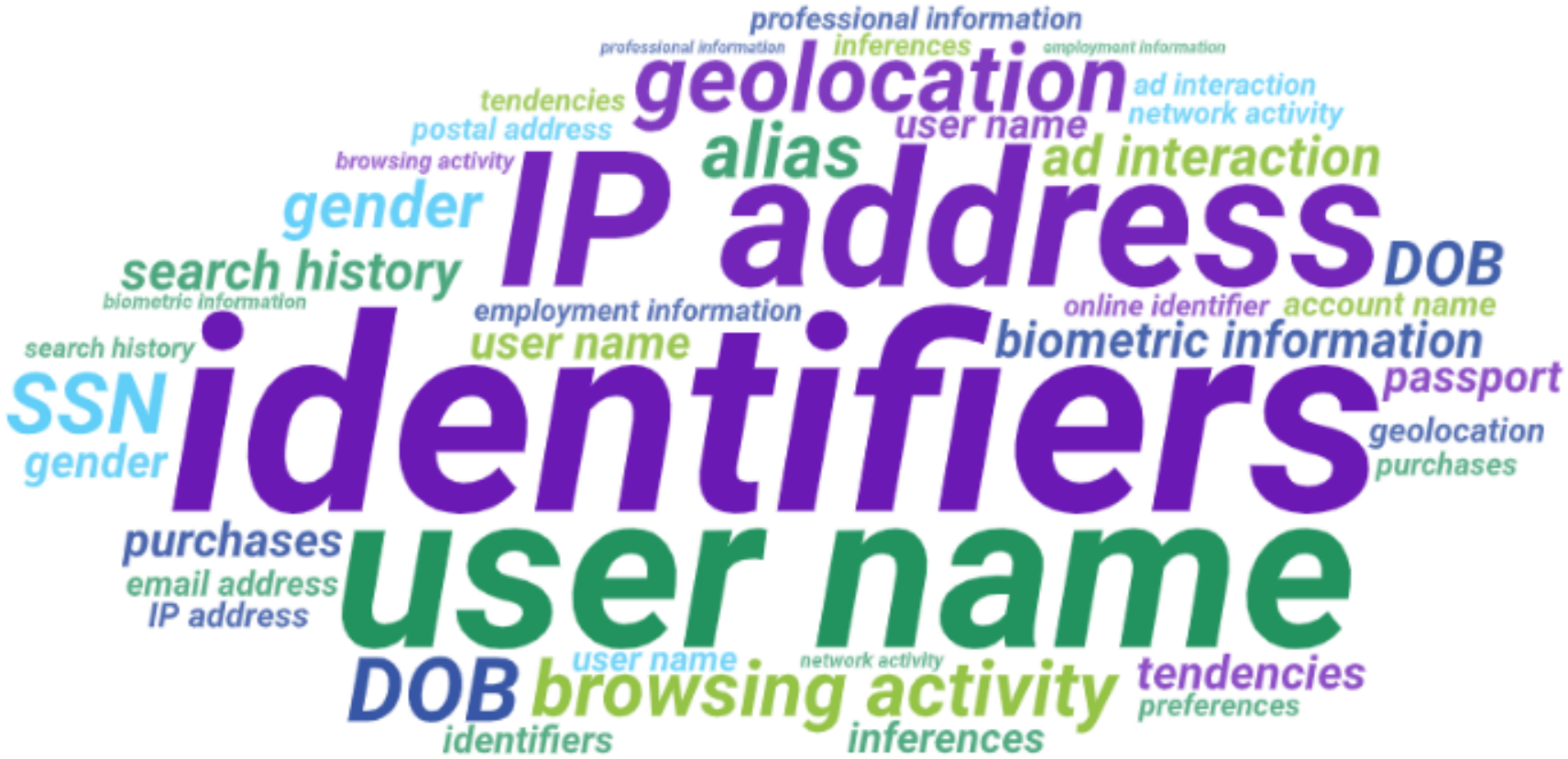
For-profit businesses that collect personal information of California residents ("consumers"), determine the purpose and means of processing of the information, and satisfy one of the following thresholds:

- $25 million in annual revenue
- Buys, receives for commercial purposes, sells, or shares the personal information of 50,000+ consumers, households, or devices
- Derives 50% or more of annual revenue from selling personal information

- Also applies to an entity that controls or is controlled by a business that meets such criteria and shares common branding

CCPA: Personal Information

Personal Information means information that identifies, relates to, or could reasonably be linked - *directly or indirectly* - with a particular consumer or household



CCPA Key Terms

- **Consumer**: A natural person who is a California resident.
  - Employees of a covered business and employees of a business which you do business are treated differently for 2020 (and perhaps longer)

- **Collect:** Buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means, including receiving information from the consumer, either actively or passively, or by observing behavior

- **Sale:** Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating, by any means, a consumer's personal information by a covered business to another covered business or third party for monetary or other valuable consideration

Business Duties under CCPA

- At / before point of collection, inform California consumers and employees of the categories of personal information collected, sources of such information, the purpose for which information is collected, and how it is shared
- Advise consumers of rights and timely respond to consumers' rights requests
- Train relevant employees
- Implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected

CCPA: Consumer Rights

Right to know

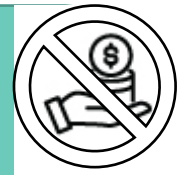
- Categories of information;
- Actual information the business has about you

Right to delete

- Delete your personal information
- Subject to exceptions

Right to opt-out ("Do Not Sell")

- Prohibit the sale or disclosure of your information to third parties (excluding service providers)



Right to not be discriminated against for exercising CCPA rights

Notice of Financial Incentive

Must provide notice of any financial incentive offered for the collection of data, and give "**a good-faith estimate of the value of the consumer's data** that forms the basis" for the offering

Employees, Applicants, Contractors, etc.

For 2020....

- Required to give own CA employees notice of what is collected and how it is used. Notice not required to be provided to employees of business customers
- No employee right of access or deletion for now
- Exemptions sunset at the end of the year *unless*...
  - California Privacy Rights Act is passed by CA voters on Nov. 2020 ballot, in which case employee and B2B exemptions are extended to 2023; or
  - Legislature passes AB 1281, which would extend exemptions until 2022

CCPA Liability and Enforcement

- Enforced by the California Attorney General
  - 30-day right to cure
  - Civil penalties **$2,500** -**$7,500** per violation
  - Enforcement began July 1, 2020

- Private Right of Action
  - Limited to instances of unauthorized access, theft, or disclosure of personal information as a result of a business's breach of its duty to reasonably protect such information
  - Greater of actual damages or **$100 - $750** statutory damages per incident
  - 30-day right to cure before initiating action (except in actions solely for actual damages)

- Nov. 2020 ballot initiative: California Privacy Rights Act

CCPA consumer cases (non-breach)

Date Filed	Plaintiff	Defendant	Court, Case No.
2/18/2020	Abhi Sheth	Ring, LLC	C.D. Cal., Case No. 2:20-cv-01538-ODW-PJW
2/27/2020	Sean Burke and James Pomerene	Clearview AI, Inc., et al.	S.D. Cal., Case No. 3:20-cv-00370-BAS-MSB S.D. Cal., Case No. 1:20-cv-03104-UA
3/30/2020	Robert Cullen	Zoom Video Communications, Inc.	N.D. Cal., 5:20-cv-02155-LHK and other related cases
4/17/2020	Heather Sweeney	Life on Air, Inc; Epic Games, Inc	S.D. Cal., Case No. 3:20-cv-00742
5/20/2020	G.R., a Minor, by and Through Her Guardian Mayra De La Cruz	TikTok	C.D. Cal., Case No. 2:20-cv-04537
6/10/2020	Bombora	ZoomInfo	Superior Court of California, County of Santa Clara
6/29/2020	Rachel Curtis, et al.	Plaid Inc.	N.D. Cal., Case No. 4:20-cv-04344

California Privacy Rights Act (CPRA) a/k/a CCPA 2.0

- CPRA is a ballot initiative sponsored by the same privacy advocacy organization who drafted CCPA
- Polling is strong; nearly 90% of people surveyed would vote YES to expand privacy protections for personal information
- Will be on the Nov. 2020 California ballot
- If passed, CPRA would be effective **January 1, 2023** – and the legislature will not be able to materially weaken its terms

Key new requirements in CPRA

Create a new category of "sensitive personal information" (SPI)

SPI is information revealing SSN or similar IDs; financial account numbers with login credentials; precise geolocation; race / ethnicity

Add new consumer rights

Right to *correct* inaccurate personal information

Right to *limit use or disclosure* of SPI

Right to *limit sharing for behavioral advertising*

Update Website homepage links

Update DNS link to "Do Not Sell or Share My Personal Information" and add new "Limit Use of My Sensitive Personal Information" link

Add new privacy principles

Expressly adopt principles of data minimization and proportionality

Extend employee and B2B exemptions

Exemption for employees and B2B expires Dec. 31, 2020; CPRA would extend the exemption 2 years until Dec. 31, 2022 – but it could deprive the CA legislature of making those exemptions permanent

Increase protections for children

Strengthen opt-in for sale or sharing for advertising; Violations when a business has actual knowledge an individual is under 16 will be subject to 3x existing fines of $7,500

CPRA would directly regulate online advertising

- Would change the definition of a covered business *from* a business that "buys, receives for the business's commercial purpose, sells or shares for commercial purposes" personal information, *to* a business that "**buys or sells, or shares**" personal information.
- Would give consumers the **right to restrict sharing of personal information for cross-context behavioral advertising**
  - "share" would be defined as sharing, disclosing, transferring, etc. a consumer's personal information to a third party for cross-context behavioral advertising, whether or not for monetary or other consideration
  - "cross-context behavioral advertising" would mean targeted advertising based on the consumer's personal information obtained from her activity across businesses, distinctly-branded websites, applications, or services, other than the business/site/app/service with which the consumer intentionally interacts
- Business would be able to avoid having the "do not sell/share" link by instead respecting consumer's opt-out preference signals sent via a browser extension, phone setting or other technology. A business could not charge more or have any consequence to a consumer to seeking to opt-out.

Additional CPRA requirements

More oversight	Transfer administrative enforcement and regulatory authority to newly formed “California Privacy Protection Agency”
More paperwork	Annual internal cybersecurity audits of sensitive processing activities
	Submission of privacy risk assessments to the CA Privacy Protection Agency “on a regular basis”
	Specified requirements for a Data Processing Agreement (DPA) when personal information is sold, shared for advertising, or disclosed to a service provider
	Prohibit future changes that would weaken California’s consumer privacy laws

Practically speaking, what would CPRA change?

Privacy Policy

- Disclose new rights
- Align categories of PI and sources to descriptions in the law

DSRs

- Operationalize right of correction and limit use of SPI
- More robust DNS functionality

Vendors / DPAs

- Service providers' may not share PI for advertising
- May add contractual requirement for monitoring or audits of vendors ~1/year

HR

- Employee rights postponed until Jan. 2023

Behavioral Advertising

- Operationalize right to limit sharing of PI to third parties for advertising

Audit

- Annual security audit of (internal) high-risk processing activities
- Potentially of service providers
- Periodic compliance reporting

CPRA Enforcement

- Private right of action still limited to data breach situations; damages unchanged
- Dual enforcement authority by the government (either/or):
  - California Privacy Protection Agency may bring an administrative action (before administrative law judge) to enforce CPRA
    - Statute of limitations is 5-years after date of violation
    - Initial probable cause proceeding may be non-public
  - California Attorney General, or local prosecutors acting on his behalf, could prosecute violations in court
- Administrative fines and civil penalties:
  - $2,500 for negligent violation
  - $7,500 for intentional violation, or for negligent violation involving PI of known minors (<16)

Litigation Response: Three Distinct Waves

Recent trends and plaintiff strategies in class actions

Holding the line on standing to sue / no harm

- Fairly successful, particularly in federal court
- Rather than prove harm, plaintiffs go in other directions
- Novel application of old laws

Key targets

- Big tech and AdTech
- Healthcare data

Recent trends and plaintiff strategies in class actions

Takeaways:

- AdTech-type claims can be asserted against anyone, and may not be linked to particular security or privacy shortcomings (most businesses are a softer target than BigTech)
- Seek early injunctions (forces immediate action; pressure for cash demands)
- Bigger focus on forum selection:
  - Favorable regions
  - State v. federal considerations
  - Diverging jurisprudence (common law)

Recent trends and plaintiff strategies in class actions

Enforcement focus

- Social media (Twitter) complaints … *today's source for news*
- Children's data … *an AG favorite*
- Healthcare data … *rarely left to HHS and the FTC*

New strategies

- Public-facing materials (including cookies, APIs, etc.)
- Leveraging CCPA requests (incl. requests to third party recipients)
- B2B suits (*e.g.,* unjust enrichment by ignoring privacy restrictions)
- Big Law willing to take on big conflicts (*e.g.,* Boies Schiller)
- Damages tactics (statutory fines, injunctions)

First wave: Data breach claims

CCPA

- New privacy rights

NY SHIELD Act

- New legal standard for cybersecurity

Wire Fraud

- B2B litigation

Common law claims

- Negligence
- Breach of Fiduciary Duty
- Invasion of Privacy

Breach of Warranty

- Access to damages

Preserving privilege of incident response and forensics

First wave: Data breach claims

Sample cases:

- *Rahman v. Marriott International, Inc.*, Case No. 8:20-cv-00654 (C.D. Cal.)
- *Atkinson et al. v. Minted*, Case No. 3:20-cv-03869 (N.D. Cal.)
- *Flynn et al. v. FCA US LLC et al.*, No. 3:15-cv-00855 (S.D. Ill.); No 20-1698 (7th Cir.)

Takeaways:

- CCPA offers the first statutory fines for data breaches, undermining lack of harm bases for dismissal and materially raising the stakes for every incident
- Anticipate more concrete threshold for "reasonable cybersecurity"

Forensic reports as work product?

In re: Capital One Customer Data Security Breach

"No difference between what [vendor] produced and what it would have produced in the ordinary course of business absent [counsel's] involvement can be reasonably inferred..."

Forensic report not privileged

"... and Capital One failed to produce evidence sufficient to establish any such likely differences"

Lessons learned

- Plan for nontraditional incidents
  - Ransomware
  - Cyber-enabled wire fraud
  - Business email compromise
  - “Data hostage” events
- Risk-based decisions (*e.g.,* more notice lowers notification risks but raises business and legal exposure risks)
- Plan ahead for cost recovery (tracking time and expenses, billing rules)
- Defensible and privileged documentation

Proactive Incident Response Checklist

- ❑ Adopt *Incident Response Plan*
- ❑ Designate internal/external response team
  - ❑ Cyber insurance
  - ❑ Legal counsel
  - ❑ Forensic support
- ❑ Backup / Disaster Recovery Planning
- ❑ Tabletop exercise
- ❑ Cybersecurity Risk Assessment / Penetration testing
- ❑ Review Privacy Policies and Regulatory Compliance (e.g., GLBA)
- ❑ Third party risk management (suppliers, clients)

Reactive Incident Response Checklist

- ❑ Initial assessment
- ❑ Initiate response
  - ❑ Involve legal team – preserve attorney-client privilege
  - ❑ Involve forensics team – preserve and investigate evidence
  - ❑ Notify insurer – preserve claims recovery
- ❑ Execute incident response plan and coordinate investigation
- ❑ Restore and remediate impacted systems and services
- ❑ Additional notifications where appropriate
- ❑ Recover costs
- ❑ Document and close incident

Second wave: Data misuse and over-collection claims

Biometrics

Patel v. Facebook (9th Cir. Aug. 8, 2019)

Vance et al suits v. Amazon (W.D. Wa., No. 2:20-cv-01084), Google (N.D. Cal., No. 5:20-cv-04696), and Microsoft (W.D. Wa., No. 2:20-cv-01082)

CCPA

Dozens of cases attempting to assert CCPA violations directly and through other causes of action (UCL, CLRA, CMIA, etc.)

CCPA consumer cases (non-breach)

The danger of wiretap claims

Cases re use of HTML and flash cookies historically resolved in favor of advertisers	• *Baxter, et al. v. Skype*, No. cv-2011-56-7 (Ark. Cir. Ct); *Baxter, et al. v. Philips Elec.*, No. cv-201105402 (Ark. Cir. Ct.) (dismissed with prejudice) • *In re: Zynga & Facebook Privacy Litigation*, Nos. 11-18044; 12-15619 (9th Cir. May 8, 2014) (disclosing unique user IDs in URLs does not violate ECPA / Wiretap Act)
Ninth Circuit revived claims that Facebook unlawfully intercepted logged-out users' browsing histories	• *In re Facebook, Inc.*, No. 17-17486, 956 F.3d 589 (9th Cir. 2020) (en banc review denied and certification likely to be sought from the U.S. Supreme Court)
Wiretap cases against healthcare providers	• *Doe II v. Tufts Medical Center Inc.*, No. 1984CV01648 (Mass. Sup. Ct. May 23, 2019) • *Doe I v. Sutter Health, No. 34-2019-00258072-CU-BT-GDS (CA Sup. Ct. Jan. 29, 2020)* • *Doe v. MedStar Health, Inc. and MedStar Good Samaritan Hospital, Inc.*, No. 24C20000 591 (Baltimore City Cir. Ct. Jan. 31, 2020)
Other cases popping up	• *Javier v. Assurance IQ*, No. 5:20-cv-02860-VKD (N.D. Cal.) (TCPA consent software) • *S.C. v. Buddi US LLC et al.*, No. 30-2020-01143611-CU-MC-CXC (CA Super. Ct., Cty of Orange) (ankle tracking bracelets) • *Russo et al. v. Microsoft Corp.*, No. 3:20-cv-04818 (N.D. Cal.) (business class action alleging Microsoft shares Office 365 data with Facebook)
New Boies Schiller wiretap cases against Google	• *Brown et al v. Google LLC et al,* No. 5:20-cv-03664 (N.D. Cal.); *Rodriguez et al v. Google LLC et al*, No. 5:20-cv-04688 (N.D. Cal.)

State wiretap laws can include statutory fines

Example	Wiretap Act Statute	Statutory Damages
California	Cal. Penal Code §§ 632, 637.2	(1) Five thousand dollars ($5,000) per violation. (2) Three times the amount of actual damages, if any, sustained by the plaintiff.
Maryland	Md. Code Ann., Cts. & Jud. Proc. § 10-402(a)(1)	(1) Actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher; (2) Punitive damages; and (3) A reasonable attorney's fee and other litigation costs reasonably incurred.
Massachusetts	Mass. Gen. Laws ch. 272, § 99F(1)	(1) Actual damages but not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1000, whichever is higher; (2) Punitive damages; and (3) A reasonable attorney's fee and other litigation disbursements reasonably incurred.
Washington	Wash. Rev. Code § 9.73.030(1)	Actual damages, including mental pain and suffering endured by plaintiffs, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation.

Wiretap claims against healthcare providers

Hospital Cases

- Key allegation: in using standard website marketing/analytics tools, hospitals are sharing website user data with Google, Facebook, etc.— who can identify users (even if hospitals cannot) —and without clear notification to users
- Particularly problematic in the healthcare context, but could be an issue in other sensitive areas as well (law firms, drug rehab, diet, dating, etc.)

Second wave: Data misuse and over-collection claims

Sample cases

- *In re: Ring LLC Privacy Litigation* (C.D. Cal.)
- *In re: Zoom Video Communications, Inc. Privacy Litigation* (N.D. Cal.)
- *Burke v. Clearview AI Inc.*, No. 3:20-cv-00370 (S.D. Cal.) (*also* Ill., NY, VA)
- *In re Facebook, Inc.*, No. 17-17486 (9th Cir. 2020), on appeal to Sup. Ct.

Takeaways:

- Misuse cases are the current BIG RISK (more than data breaches) both in terms of damages and injunction risks; companies cannot play the victim
- Concerned about courts manufacturing new "common law" duties
- AdTech-type claims not linked to particular security or privacy shortcomings

Third wave: Data ownership and civil rights

Whose data is it?

Property rights on intangible assets

Risk of common law “data fiduciary” decision

AI, bias and social justice

CCPA → CPRA → what’s next?

Third wave: Data ownership and civil rights

Legislation	Data broker laws	Bias and discrimination
• Draft state and federal bills impose fiduciary duty on businesses, e.g., *Data Accountability and Transparency Act of 2020* by Sen. Sherrod Brown (D-OH)	• Vermont • California	• *HUD v. Facebook*

Takeaways:

- A few cases have endorsed data ownership concept
- Change in party control next year could heavily impact laws/enforcement risk
- National privacy debate of property rights v. inalienable civil rights
- Could potentially involve highly-charged societal issues

Artificial intelligence: current legal framework

Law governing evolving AI technology is unsettled

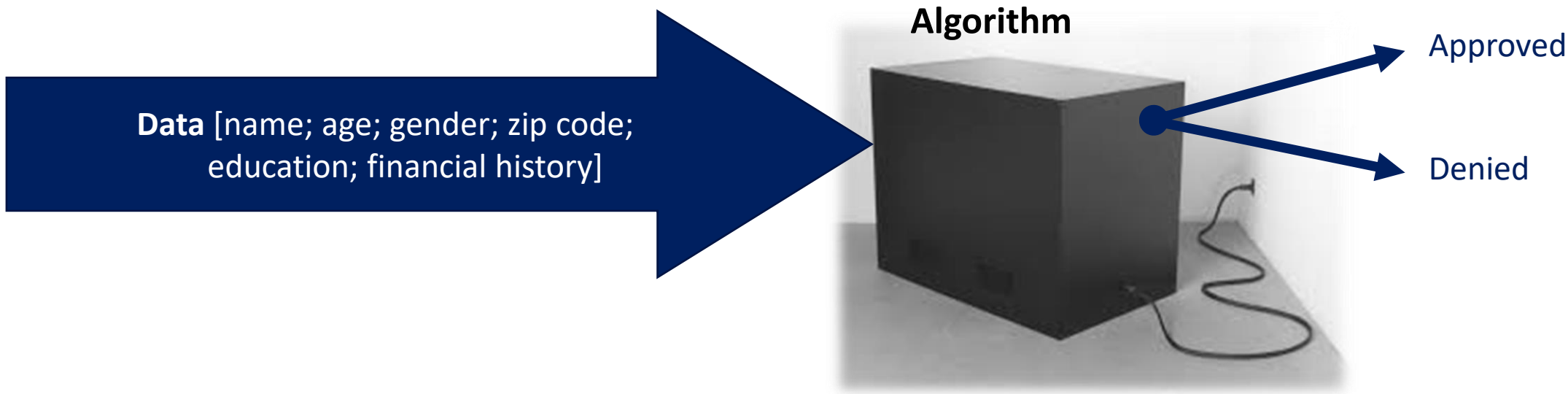
- No clear legal standard across all AI
- Over 40 bills that address AI have been introduced in Congress level)
- Legislators and regulators reluctant to act fast: don't want to stymie development of AI
- Opted for principles, guidance, statements
- Most experts believe the laws already in place for human activity that AI replaces can equally apply to developing technologies

Select AI liabilities theories: common law & statutory

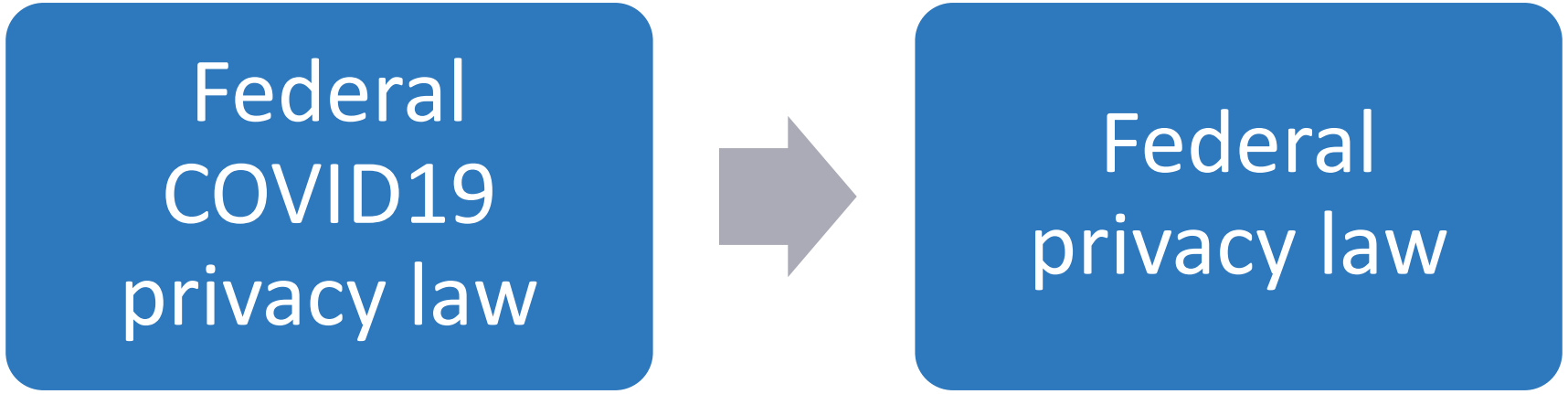
Products liability	Negligence / Malpractice	Vicarious Liability / Respondent superior	FTC Act	FCRA	CRA
• Addresses liability for manufacturers and developers* permitting *recovery when* injured by products that are "not reasonably safe" due to defective design, manufacture, or warning. • Foreseeability and failure to warn key basis for liability.	• Addresses liability for developers, manufactures, users when conduct falls below the established standards of care. • Duty of care judged against those in a similar position with the same knowledge, skills, and expertise—under like circumstances.	• Addresses employer and agent liability for negligent acts of employees acting within the scope of their employment. • Failing to exercise due care in hiring, training, or supervising employees, or for failing to maintain adequate facilities and equipment.	• Section 5 of FTC Act, 15 U.S.C. § 45(a)(1) • Prevents unfair or deceptive acts or practices in or affecting commerce.	• Fair Credit Reporting Act, 15 U.S.C. §§1681 - 1681x • Sets notice, investigation, and accuracy obligations associated with consumer reports from CRAs. • When dealing with employment or credit decisions based on a multitude of factors and predictive analytics – its obligations may be implicated.	• Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000e (2014) • Prohibits discrimination in public accommodations engaged in interstate commerce on the basis of race, color, religion, or national origin.

Issue spotting: risk of legal bias

- "Digital Redlining" – disparate impact based on decision making that is biased (creates or perpetuates inequality)
  - *E.g., HUD Charges Social Media and Technology Company, Facebook, With Housing Discrimination Over Company's Targeted Advertising Practices (March 28, 2019).*



Other issues on the horizon



Consistent disagreements on:

- Preemption
- Private right of action

Contact

Mark S. Melodia
Holland & Knight LLP
New York, NY
212-513-3583
Mark.Melodia@hklaw.com

Ashley L. Shively
Holland & Knight LLP
San Francisco, CA
415-743-6906
Ashley.Shively@hklaw.com

Anthony J. Palermo
Holland & Knight LLP
Tampa, FL
813-227-6320
Anthony.Palermo@hklaw.com

HK

Data Strategy, Security & Privacy

Cybersecurity Law Report
An Acuris company

cslawreport.com

June 10, 2020

PRIVILEGE

After Capital One Ruling, How Will Companies Protect Forensic Reports?

By Matt Fleischer-Black, *Cybersecurity Law Report*

The federal court in Virginia overseeing the multi-district litigation (MDL) against Capital One Financial Corp. has ordered the company to release the attorney-supervised forensic report that a cybersecurity firm made following the company's massive 2019 data breach. The company had claimed that work-product protection shielded the post-breach report because its outside lawyers from Debevoise & Plimpton had initiated, directed and received the analysis as part of that firm's own investigation about the breach.

Capital One argued that "the Mandiant Report is core opinion work product prepared to help counsel develop its legal theories about the Cyber Incident and strategy for defending litigation" and "should be protected as inviolate."

In its May 26, 2020 order, The U.S. Court for the Eastern District of Virginia concluded instead that Capital One had failed to distinguish Mandiant's post-breach forensic report from what the cybersecurity consultancy would have delivered without litigation looming. The Court ordered the bank to turn over the report to plaintiffs within 11 days.

The ruling is a warning that businesses cannot count on a series of earlier rulings that shielded forensic reports as privileged, Mark Melodia, a Holland & Knight partner, told the Cybersecurity Law Report. "Most of the time in breach litigation, [the protection of forensic reports has] not been a big subject of debate," he said, adding, "Maybe we've gotten a little complacent assuming and thinking that protection will be there."

See "Increased Post-Breach Discovery Turns Spotlight on Privilege" (Mar. 20, 2019).

Debevoise's Steps to Establish Privilege

Capital One hired Debevoise on July 20, 2019, immediately after discovering that cyber attackers had exposed the sensitive data of over 100 million individuals. Debevoise directly retained cybersecurity consultant Mandiant to help the law firm prepare for a tide of litigation. A few days later, the Virginia-based bank announced the data heist, and consumers filed a wave of lawsuits, since consolidated into an MDL.

Debevoise took several steps to cover Mandiant's investigation under its own protected work product. Debevoise's engagement letter specified that it would direct and receive Mandiant's work to render legal advice for litigation. Capital One paid for

the work from its legal budget (after a delay). The bank partitioned off the Mandiant team from its own cyber team's investigation into the breach, Capital One said. The bank has not claimed privilege over that second set of investigative materials, court documents show.

Once Mandiant delivered its report, Debevoise restricted its distribution to Capital One's legal team, which later shared the report with relatively few non-lawyers at the company. In sum, "all of the circumstances surrounding the creation of the Mandiant report support the conclusion that the Mandiant Report is protected work product," the company argued.

See "Capital One Breach Demonstrates Risk of Overlooking Vulnerabilities When Sending Data to the Cloud" (Aug. 14, 2019).

The Court's Rejection of Work-Product Immunity

Not Enough Evidence It Was Molded by Litigation

The privilege standard will protect work product like the cybersecurity firm's breach report, the order noted, only when the document distinctively reflects preparation for litigation. Capital One had a burden to distinguish the forensic analysis's content from what would appear in a report issued for a pure operational purpose, if a lawsuit was not an issue.

Looking for factors to make that distinction, the Court instead saw a paper trail showing similarity. Capital One first hired Mandiant in 2015, paying the cybersecurity company an annual retainer for 285 hours of work after an incident, which it labeled a "business-critical" expense, not a "legal" one. Capital One's "regular business" agreement, entered into before the incident, and a Debevoise-drafted "litigation" contract executed after the breach looked functionally the same, the Court said. It concluded that the bank had "effectively transferred" its Mandiant agreement to outside counsel.

The Court saw two other indicators of a superficial handover of a business function. The bank initially paid Mandiant's post-breach fees with its existing retainer, only later adjusting its budget attribution to legal. Capital One also supplied the Mandiant forensic report to the bank's outside auditor and four different regulators, which the Court regarded as business purposes.

See "Preserving Privilege in Audits and Internal Investigations" (Jun. 3, 2020).

Describing Mandiant's Technical Work Colorlessly

Debevoise's descriptions did not persuade the Court that Mandiant's breach analysis touched sufficiently on legal elements, impressions, or other traditional markers that merit work-produce immunity. The firm's agreement with Mandiant characterized the consultant's assistance as "computer security incident response," "digital forensics, log, and malware analysis," and "incident remediation."

Debevoise said in a court declaration that Mandiant had helped the law firm give legal advice by (i) aiding its grasp of "technical matters in documents the firm reviewed and certain witness interviews it conducted;" (ii) "conducting targeted sub-investigations on technical matters related to the incident;" and (iii) performing a "red team exercise to assess

remediation" of the vulnerability that enabled the breach.

The Court concluded that the work resembled what Mandiant would have provided Capital One were the bank immune from lawsuits, and ordered disclosure, citing the law's aversion to blanket evidentiary exclusions that limit truth-seeking.

See "Lessons From SDNY Ruling on How to Preserve Privileged Communications With Attorney Consultants" (Aug. 7, 2019).

Legal Landscape

Second Straight Skeptical Ruling in Virginia Federal Court

The Capital One decision adds to a string of rulings denying privilege for consultants' data breach reports. The Court invoked a December 2019 case, *In re Dominion Dental Services*, that refused to protect a Mandiant post-breach forensic incident report. The Court also cited the *In Re Premera Blue Cross* rulings from Oregon's federal court (2017 and 2019). In *Premera*, as in the Virginia cases, Mandiant had worked for the company before the breach, providing a paper trail. This continuity of relationship colored each court's conclusion that, in total, Mandiant's work did not materially change when outside counsel became involved.

The Virginia and Oregon courts did not address First Amendment issues, though in 2019, a Maryland court ordered Marriott to release a forensic analysis of a large breach it suffered on First Amendment access grounds.

Circuit Split

The *Capital One* order weighed four contrary opinions in other jurisdictions that held that the work-product protection applied to forensic reports addressing data breach incidents experienced by Arby's, Target, Experian and Genesco. The Court discounted some of these precedents, Melodia noted, for being too perfunctory to offer guidance. In contrast, the opinions that the Court relied upon include detailed analyses. "Judges who decide not to provide the protection seem to feel compelled to write more because they are going against the grain," he observed.

Overall, "published decisions and publicly available law still clearly favor protection of forensic reports as work product," Melodia said. When one accounts "for all of the instances when the privilege question has been decided on a conference call, or in a short letter opinion from a magistrate judge, or where it has been on a privilege log and plaintiffs' counsel accepted that without dispute," the argument for granting privilege is even stronger, he contended.

Plaintiffs' attorneys, however, also point to instances where businesses disclosed the reports without published orders. In the Dominion case, plaintiffs' pleadings cited Anthem and Excellus each turning over forensic incident reports without dispute in their data breach class actions.

"We have a variety of opinions now on this topic," noted Paul Luehr, a partner at Faegre Drinker Biddle, and "it's difficult to anticipate how much weight will be put on this particular decision."

One lesson of *Capital One* for companies defending themselves, Melodia offered, is that companies should ask courts that grant protection to forensic reports to write a detailed order explaining their rationales. These courts may not think analysis is necessary, he said, because "they are simply doing what everybody assumes would be done" in extending immunity to such reports.

See "*Target* Privilege Decision Delivers Guidance for Post-Data Breach Internal Investigations" (Nov. 11, 2015).

Preserving Privilege After the *Cap One* Decision

Show the Court More Legal Involvement – Carefully

Courts weighing privilege claims want to know whether "the report was seen and reviewed and revised by counsel. Was it actually done for counsel to be able to give the company legal advice or not?" said Arnold & Porter partner Jami Mills Vibbert, who noted that she could not discuss the Capital One case specifically.

To better satisfy the reviewing court, companies could share details about the lawyers' process around the report. These could include, Melodia suggested, "how often the forensic team checked in with and received direction from the legal team, the framing of the work by the legal team with an eye on legal risks and requirements, and the ways in which the report reflects the joint work product of technical and legal professionals."

Also, lawyers could go beyond the boilerplate in the engagement letter – such as, "the work will be directed by counsel and is intended to help provide legal advice" – to include process expectations and incident specifics.

The downside of discussing process, Melodia said, is that "it could provide a roadmap" for plaintiffs "if anybody involved in the investigation is deposed." The attorneys must not be too effusive, Melodia cautioned. "To put a lot of legal-team fine points into the statement of work or the engagement letter is really risking subject-matter waiver," he explained. Plaintiffs' attorneys will then ask to see "your other documents and your thinking about these five specific legal issues that you've raised," he added.

See "Attorney-Consultant Privilege? Key Considerations for Invoking the *Kovel* Doctrine (Part One of Two)" (Nov. 16, 2016); Part Two (Nov. 30, 2016).

Fold the Forensic Report Into an Appendix

Capital One and the string of decisions before it are stoking fears that lawyers' and forensic investigators' candid conversations could be used against them in court. "If this decision were to be the standard, it discourages a probing forensic analysis of data incidents and committing that work to writing at a most basic level," Melodia said.

Instead, companies and their outside counsel could instead prepare a blended investigative report for the data breach, Vibbert advised. "The best practice is to restrict the forensic material to an appendix for the attorney's investigative report," she suggested.

The appendix would include only the factual findings and details, like log evaluations. With

this approach, the outside counsel folds the rest of the forensic details into the legal advice and discussions in the body of the memo, Vibbert explained.

See "Preserving Privilege Before and After a Cybersecurity Incident (Part One of Two)" (Jun. 17, 2015); Part Two (Jul. 1, 2015).

Ask for In-Camera Review

Whether in an appendix or not, the plaintiffs likely will seek the disclosure of the forensic analysis. Judges in prior cases conducted *in-camera* reviews to evaluate whether a report deserved work-product immunity, Melodia noted. If a judge seems skeptical, defense counsel may ask the judge to review the report to verify the lawyers' handiwork. "That's a better option than receiving an opinion in a vacuum, which maybe makes certain assumptions about the memo that aren't true," he said.

Best Practices Despite the Decision

Don't Wait for a Breach to Hire a Forensic Firm

Among the worst implications of recent decisions like *Capital One*, *Dominion* and *Premera*, Melodia and Luehr agreed, is the preference they seem to afford to companies that hire new forensic experts after the breach. Each decision cited details from the companies' ongoing business relationship with Mandiant as a key factor in their evaluations, Luehr explained. "Then they contrasted that with precedents where the defendants hired teams at the last minute" as clearer scenarios for earning privilege, he added.

This preference for establishing a new forensic relationship post-breach, Luehr cautioned, threatens to undermine a central, best practice in cybersecurity – being ready to respond rapidly. "The GDPR and the New York DFS regulation are pushing companies to report breaches within 72 hours, yet this decision suggests that companies should spend most of that precious time trying to find and sign up a forensic expert at the last minute," he said.

The Court's emphasis, Melodia agreed, "is particularly off base in the financial services industry, where a thorough vetting of vendors is an absolute regulatory requirement through the Fed and OCC and a lot of state banking regulators," he said. "Third-party oversight rules are very demanding. You can't bring just anybody in to start working on the bank's innermost data systems, which contain personal information," he added.

Hiring a new incident response firm post breach is inefficient, risky and costly, Melodia noted. "I've seen investigations held up a week or more at the outset because of contract negotiations or fees," he recalled. During that time, "you are potentially losing evidence, potentially allowing intrusion to continue and potentially delaying engagement with law enforcement," he warned.

Retaining a firm in advance is also prudent, Luehr said, to prepare for a spread of ransomware or times of elevated assaults, as in the current pandemic. Those situations create a run on experienced responders. He recalled instances he has observed "where those who did not make that forensic hiring decision and retention in advance [were] left on the outside looking in," without a trusted consultant.

See "A Roadmap to Preparing for and Managing a Cyber Investigation" (Nov. 14, 2018).

Lawyers Should Keep Setting the Forensic Agenda

The *Capital One* decision is out of step with the prevailing reality of forensic investigations after an incident, Luehr noted. It gives the impression that lawyers and forensics investigators work separately – as if the lawyers unlock the work room, hand over admin passwords, then let the forensic team alone to burrow into the logs and networks.

In practice, "the forensic report that most experts generate is driven almost exclusively by the law," Luehr said. The outside counsel asks the cybersecurity consultants to look for details that clarify whether the company must notify affected individuals, regulators and the markets.

Focusing the forensic investigators may require some pushing, as they intuitively are "interested in how the attackers got in and how you button up that hole. Often, they want to fix the problem and move on," Luehr said. Without a lawyer's urging, "they would not pay attention to PII or what jurisdiction affected people are in," he added.

Vibbert agreed that the law firm must guide the forensic team, for example, to ensure review of a broad enough array of data categories. "It's not the forensic investigator's job to know that certain terms have legal meaning and may be construed as evidence," she said. It is hard to imagine that this decision will lead to lawyers pulling back from working closely with forensic analysts. Without cooperation with forensics, lawyers will be unable to quickly determine the company's obligations and will not be able to properly notify regulators and business partners.

The collaboration of legal and forensics professionals is crucial for evaluating the litigation risk, Luehr said, as they assess the history of the company's defenses and "how far along the company was in its maturity journey to reasonable security." Focal points that merge technical and legal questions, Melodia added, include whether a breached company's staff ignored red flags, lacked a proper protocol, or were using last year's best practices instead of this year's.

See "Answers to Four Critical Questions on Privilege in Internal Investigations" (Dec. 5, 2018).

Keep Collaborating Closely Post Breach

The *Capital One* opinion, Melodia lamented, undercuts the hard-won learning of the past decade about how to best respond to a breach. "It goes back to the day when there were very siloed individual experts after an incident," he said.

"It used to take a long time and a lot of work," for the different professionals to investigate separately, Melodia recalled. The various players had to figure out how to talk to each other, protect the company's different interests, synthesize the risks into a clear picture and eventually decide on a response. The delay hurt both sets of victims – the company and the affected individuals, he noted. "It's taken more than a decade for the clients to understand how the response is a team sport," he recalled.

Debevoise told the Court that it had conducted 160 interviews. Melodia observed that, if the investigation were "as thorough and deep" as

that sounds – cautioning that he had not seen more details – the lawyers likely had shaped the forensic work. Capital One's counsel and the plaintiff's lawyers did not reply to requests for comment about the collaboration, evidence available to the Court and Debevoise's work product.

See our three-part series on protecting attorney-client privilege and attorney work product while cooperating with the government: "Establishing Privilege and Work Product in an Investigation" (Feb. 8, 2017); "Strategies to Minimize Risks During Cooperation" (Feb. 22, 2017); and "Implications for Collateral Litigation" (Mar. 8, 2017).

Is It in the Public's Interest to Expand Privilege?

If we see more decisions like this, Vibbert and Melodia agreed, companies may start to pursue more protection from courts for breach planning and response. A December 2019 report from the Sedona Conference laid out the case for a qualified privilege for cybersecurity information prepared both before and after security events. "You want companies to laser-focus on stopping the bleeding, not to think about the liability that might arise because of the attack," said Vibbert, who helped prepare the report.

"In most companies' incident response plans," Vibbert noted, "the first call is to the lawyers, because of liability issues. But that slows down the provision of information" to law enforcement and regulators, which hurts the overall response.

Companies could start citing this white paper in filings to courts or ask legislatures and courts to extend protection in evidentiary rules, Vibbert said. "Because the attacker is, in many cases unknowable, and the entity on the hook is the victim of the crime, this is a unique circumstance and we could have a public policy of affording more protection when a company finds out about a security incident," she argued. The Cybersecurity Information Sharing Act of 2015 may persuade authorities to consider the idea.

Attorney oversight of every aspect of the forensic investigation and the creation two separate teams is expensive and misplaces priorities, Vibbert added. "The thing companies should not be doing first is trying to protect documents," he said.

Holland & Knight

ALERT

Litigating the CCPA in Court

July 22, 2020

Mark S. Melodia
Ashley L. Shively
Mark H. Francis
Paul Thompson Jr.

HIGHLIGHTS:

- Despite significant restrictions on private rights of action, more than 50 lawsuits have invoked the California Consumer Privacy Act (CCPA) since it took effect on Jan. 1, 2020, nearly all of them class actions.
- While the CCPA is expected to play an important role in future data breach cases given the availability of statutory damages, plaintiffs' right to litigate alleged CCPA violations in other contexts will face strong opposition, and this may be the most important CCPA issue in the coming six to 12 months.
- With the California Attorney General's enforcement activities beginning on July 1, 2020, businesses need to manage potential liability exposure on two fronts, and it is currently unclear which front will pose the bigger risk.

The California Consumer Privacy Act (CCPA or Act) went into effect on Jan. 1, 2020. A first-of-its-kind law in the United States, the CCPA grants California residents expansive rights over businesses' collection, use and sharing of their personal information. The Act provides California residents with the right to seek access to, or deletion of, their personal information, as well as the right to object to the sale or sharing of such information with third parties.

For the most part, the CCPA vests enforcement authority with the California Attorney General (CA AG),[1] and certain critical compromises were struck during the CCPA's dramatic legislative process in 2018 and 2019 to limit private enforcement for other violations:

- *First*, the law expressly provides that a private right of action is available only for certain data breach incidents "and shall not be based on violations of any other section of" the CCPA. The Act further states that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law."[2]
- *Second*, although data breach suits may be brought on an individual or class-wide basis for actual damages incurred or statutory damages,[3] a consumer seeking statutory damages must first provide the intended defendant with 30 days' advance written notice of the alleged violations of the CCPA, and if the business cures the alleged violation and provides an express written statement to that effect, the would-be plaintiff may not initiate an action for statutory damages.[4]

Many requirements of the CCPA have been the subject of legal debate since the law passed, and the precise contours of enforcement has been a popular topic.[5] There was, however, generally broad consensus that consumers would swiftly embrace the availability of statutory damages, and, be equally quick to challenge the limits of the CCPA's private right of action. It is therefore no surprise that in the seven months since the CCPA went into effect, approximately 50 private lawsuits have been filed that cite the CCPA in some respect as a basis for suit.

Roughly half of these lawsuits were filed in connection with data breaches. Plaintiffs in the other cases premise claims on alleged violations of consumer rights, often asserting that noncompliance with the CCPA, by extension, constitutes a violation of California's Unfair Competition Law (UCL), Consumer Legal Remedies Act (CLRA) or other causes of action. Unsurprisingly, these suits are generally filed as class actions.

CCPA Suits Filed in Connection with Security Incidents

The CCPA adds an attractive new dimension to data breach class action cases. Plaintiffs have traditionally struggled to establish that a particular security incident was the proximate cause of monetary damages or some other actual injury recognized by law. This hindered plaintiffs' ability to establish Article III standing in federal court and present a viable damages theory. The CCPA is the first generally applicable data breach law in the United States to offer statutory damages as an alternative to establishing actual damages.

In the new wave of CCPA data breach cases, plaintiffs have generally pleaded a right to statutory damages, and also often seek restitution and an injunction against defendants' continued (allegedly) improper handling of personal information.[6] Only a small percentage of cases allege actual damages as a result of the purported incident.[7]

The data breach lawsuits plead violations under the CCPA with various degrees of specificity. Most cases allege a data breach and then generally contend that the breach was a violation of the CCPA without offering further detail.[8] In this context, the CCPA claim is typically asserted along with other common data breach claims including negligence, breach of contract, unjust enrichment and violation of the UCL.[9]

Other cases are pleaded with greater specificity and allege that the plaintiffs gave the defendant notice prior to filing suit.[10] In at least several instances, however, it does not appear that plaintiffs waited the requisite 30 before filing suit.[11]

A number of cases also assert a violation of California's UCL *based on* a violation of the CCPA arising from a data breach.[12] The UCL defines "unfair competition" broadly to "mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by [California's false advertising law]."[13] Private parties may seek injunctive relief and restitution under the UCL.[14] These claims, therefore, necessarily seek validation from the courts that the UCL is an appropriate vehicle through which an underlying CCPA violation can be asserted in a private action (this is discussed further below).

CCPA Suits Unrelated to Security Incidents

Notwithstanding the CCPA's narrow private right of action, a variety of other lawsuits have been filed alleging violations of the law.

Violations of the Notification Requirements

The plaintiffs in several recently filed lawsuits have brought claims directly under the CCPA for alleged violations of the Act's notification requirements.[15] In these cases, the plaintiffs typically allege that the defendants' website or application collected more personal information than was disclosed and/or used consumers' personal information in a manner that was inconsistent with the representations in the defendants' privacy policy. The plaintiffs often seek injunctive relief and actual damages.[16] For example, one complaint provides that the defendant's app prompted the plaintiff to connect the app to her social media account.[17] Once connected, the defendant allegedly shared the plaintiff's personal information collected while she used the app with the social media platform. The plaintiff further alleges that such sharing occurred without the notification required under the CCPA.[18]

Claims such as these outright ignore the CCPA's restriction that a consumer may only bring a private right of action for certain data breaches.

UCL Claim Premised on Violation of the Notification Requirements

In other cases, plaintiffs have pleaded their claims under the UCL, premised on alleged violations of the CCPA's notice requirements.[19] Plaintiffs in these cases essentially argue that a CCPA violation is a *de facto* violation of the UCL.[20] For example, one complaint alleges that the defendant "scraped" hundreds of websites for consumers' personal information (which the defendant later sold) without consent and in violation of the CCPA's notification requirements.[21] The plaintiffs proceed to argue that a violation of the CCPA's notification requirements, is by extension, a violation of the UCL.[22] As with the UCL data breach claims, UCL claims premised on alleged notification violations thus implicitly seek judicial approval to expand CCPA enforcement — notwithstanding the Act's clear instruction that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law."[23]

Claims Alleging General Violation of Privacy Rights

Other cases avoid making a claim under any specific provision of the CCPA; plaintiffs instead plead facts regarding a defendant's use of personal information and allege a violation of state privacy rights, for instance under the California Constitution.[24] In one such case, the plaintiffs seek an injunction, and to the extent that the defendant fails to respond to the plaintiffs' letter giving notice to CCPA violations, the plaintiffs also seek actual, punitive and statutory damages, restitution, and attorneys' fees and costs.[25] Similar to the UCL-based claims, these claims appear to invite the courts to rely upon the CCPA as a vehicle to establish privacy standards for which liability can be justified under other applicable laws.

All of these claim theories venture into unchartered territory. These cases continue to be filed and as they work their way through California's federal and state courts, it remains to be seen how judges will rule on motions to dismiss such claims.

Asserting Violations of the CCPA in Business-to-Business Litigation

Class action plaintiffs do not have a monopoly on creativity. One recently filed case is between competing businesses engaged in market research that involves the collection and sale of personal information.[26] The plaintiff alleges that the defendant (the plaintiff's former business partner and now competitor) violated the CCPA by failing to provide sufficient notice of its privacy practices to consumers, and as a result, has gained an unfair and unlawful advantage in violation of the UCL. The plaintiff is seeking restitution, disgorgement and an injunction against its competitor.

Using the CCPA as a weapon in the business context could give rise to a whole new field of CCPA litigation. One can imagine litigious businesses leveraging the CCPA in a manner similar to false advertising claims, or plaintiffs raising the CCPA in whistleblower suits, or shareholder derivative and securities class actions, alleging noncompliance with the Act to the detriment of employees, shareholders or to the value of the defendant business itself. The viability of such claims — purportedly on behalf of the consumers that the law is intended to protect — would seemingly require an extension of legal doctrine equal to, or greater than, in the consumer cases described above.

The CCPA "Safe Harbor" Defense

In January 2019, the City of Los Angeles filed suit against The Weather Channel (TWC).[27] In the complaint, the City alleged that TWC was engaged in unfair and fraudulent business practices in violation of the UCL by sharing its mobile app users' geolocation data with third parties for advertising and other commercial purposes, without providing sufficient notice or obtaining any necessary consent.

On June 11, 2020, TWC filed a motion for summary judgment,[28] arguing that the City's "lawsuit is an improper attempt to legislate through litigation."[29] The disclosure requirements advocated for by the City, TWC contends, "significantly *exceed* and *conflict with* the highly detailed and rigorous disclosure requirements imposed under CCPA . . . which [moreover] did not go into effect until a year *after* Plaintiff filed suit."[30] Rather than permitting UCL-type claims over what constitutes appropriate notice to consumers of a business' privacy practices, TWC urges the court to defer to the state legislature "which has already decided these questions—so that California businesses (and others doing business in California) are able to know, to a reasonable certainty, what conduct California law prohibits and what it permits."[31]

Privacy practitioners heavily engaged on CCPA compliance matters may well see a paradox in any argument that the CCPA provides "reasonable certainty" regarding California's required privacy disclosures. But perhaps over the next one to two years the courts (or the regulator . . . whoever that may be) will provide that clarity — there is no doubt they will have many opportunities to do so.

Notes

[1] See Cal. Civ. Code § 1798.155(b).

[2] See Cal. Civ. Code § 1798.150(c) ("The cause of action established by this section shall apply only to violations as defined in subdivision (a) [regarding data breaches] and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.").

[3] Statutory damages range from $100-$750 per individual, per incident. Cal. Civ. Code § 1798.150(a)(1)(A).

[4] See Cal. Civ. Code § 1798.150(b).

[5] There is some debate, for instance, over whether county or local prosecutors in California can bring public enforcement actions for violations of the CCPA under Section 17204 of California's Business and Professions Code, or if enforcement is *solely* vested with the CA AG.

[6] See, e.g., Complaint, *Jose Lopez v. Tandem Diabetes Care, Inc.*, No. 3:20-cv-00723-LAB-LL, at 25 (S.D. Cal. April 16, 2020).

[7] See, e.g., Complaint, *Lopez*, at 25; Complaint, *Fuentes v. Sunshine Behavioral Health*, No. 8:20-cv-00487, at 20-21 (C.D. Cal. March 10, 2020) (alleging that the data breach caused the plaintiffs harm as they must now "freeze" credit cards, contact financial and health institutions, monitor credit reports, etc. for "years to come").

[8] See, e.g., Complaint, *Albert Almeida, Mark Munoz, and Angelo Victoriano v. Slickwraps Inc.*, No. 2:20-at-00256, at 28, 48 (E.D. Cal. March 12, 2020); Complaint, *Daniela Hernandez v. PIH Health*, No. 2:20-cv-01662, at 6, 19, 38 (C.D. Cal. Feb. 20, 2020); Complaint, *Bernadette Barnes v. Hanna Andersson, LLC, and Salesforce.Com, Inc.*, No. 4:20-cv-00812-DMR, at 3, 15 (N.D. Cal. Feb. 3, 2020); Complaint, *Juan Maldonado v. Solara Medical Supplies, LLC*, No. 3:19-cv-02284-H-KSC, at 3, 21 (S.D. Cal. Nov. 29, 2019).

[9] See, e.g., Complaint, *Slickwraps* at 39, 44, 46 and 48; Complaint, *Hernandez* at 22, 27, 30 and 37; Complaint, *Barnes* at 16 and 22; Complaint, *Maldonado* at 23, 30, 33 and 34.

[10] See, e.g., Complaint, *Michele Pascoe v. Ambry Genetics*, No. 8:20-cv-00838, at 50 (C.D. Cal. May 1, 2020) at 50; Complaint, *Lopez* at 44.

[11] Complaint, *Lopez* at 44 ("***If*** Defendant fails to respond to Plaintiffs' notice letter or agree to rectify the violations detailed above, Plaintiffs also will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations.") (emph. added)

[12] See, e.g., Complaint, *Slickwraps* at 48; Complaint, *Hernandez* at 37-38.

[13] See Cal. Bus. & Prof. Code § 17200.

[14] See *Am. Bankers Mgmt. Co., Inc. v. Heryford,* 885 F.3d 629, 632 (9th Cir. 2018).

[15] See, e.g., Complaint, *G.R. v. TikTok*, No. 2:20-cv-04537, at 9 (C.D. Cal. May 20, 2020); Complaint, *Sweeney v. Life on Air*, No. 3:20-cv-00742, at 21 (S.D. Cal. April 17, 2020).

[16] See e.g., Complaint, *TikTok* at 10; Complaint, *Sweeney* at 22.

[17] See Complaint, *Sweeney* at 3-4.

[18] See *Id.*

[19] See, e.g., Complaint, *Sean Burke and James Pomerene v. Clearview AI, et al.*, No. 3:20-cv-00370-BAS-MSB, at 22 (S.D. Cal. June 14, 2020); Complaint, *Cullen v. Zoom*, No. 5:20-cv-02155-LHK, at 12 (N.D. Cal. March 30, 2020).

[20] See, e.g., Complaint, *Burke* at 24; Complaint, *Cullen* at 14.

[21] Complaint, *Burke* at 2-4, 11-13, 14-17, and 22-24.

[22] See *Id.* at 22-24.

[23] Cal. Civ. Code § 1798.150(c).

[24] Complaint, *Sheth v. Ring*, No. 2:20-cv-01538-ODW-PJW, at 11 (C.D. Cal. Feb. 18, 2020).

[25] *Id*. at 20-21.

[26] See Complaint, *Bombora v. ZoomInfo*, No. 20-cv-365858 (Cal. Super. Ct. June 10, 2020).

[27] See Complaint, *California v. TWC Prod. and Tech., LLC*, No. 19-STCV-00605 (Cal. Super. Ct. Jan. 3, 2019).

[28] Due to the COVID-19-created backlog in the court, TWC's motion is not set to be heard until February 2021.

[29] Defendants' Notice of Motion and Motion for Summary Judgment on Defendants' Affirmative Defense of Equitable Abstention, *California v. TWC Prod. and Tech., LLC*, No. 19-STCV-00605, at 1 (Cal. Super. Ct. June 11, 2020).

[30] *Id*. at 2 (emphasis in original).

[31] *Id*. at 20 (quotation omitted).

Authors

Mark S. Melodia
New York
212.513.3583
mark.melodia@hklaw.com

Ashley L. Shively
San Francisco
415.743.6906
ashley.shively@hklaw.com

Mark H. Francis
New York
212.513.3572
mark.francis@hklaw.com

Paul Thompson Jr.
Boston
617.305.2174
paul.thompson@hklaw.com

Holland & Knight

Mark S. Melodia

PARTNER

Mark.Melodia@hklaw.com

New York
212.513.3583

PRACTICES
Data Strategy, Security & Privacy | Class Action Litigation and Arbitration | Litigation and Dispute Resolution |
Global Cybersecurity and Privacy Policy and Regulation |
Intellectual Property | E-Commerce |
Consumer Protection Defense and Compliance | Healthcare & Life Sciences | Financial Services | Financial Services Litigation | Israel Practice |
Digital Healthcare

INDUSTRIES
Technology & Telecommunications | Healthcare & Life Sciences

Mark Melodia is a privacy, data security and consumer class action defense lawyer in Holland & Knight's New York office and serves as the head of the firm's Data Strategy, Security & Privacy Team. Mr. Melodia focuses his practice on governmental and internal investigations, putative class actions and other "bet-the-company" suits in the following areas: data security/privacy, mortgage/financial services and other complex business litigation, including defamation.

Mr. Melodia has defended more than 90 putative class actions – including as lead defense counsel in multiple multidistrict litigations (MDLs) – arising from alleged consumer privacy violations, data incidents and allegations of data misuse. He routinely represents clients responding to government privacy investigations before the Federal Trade Commission (FTC), Office for Civil Rights, state attorneys general and the U.S. Department of Justice (DOJ). He has guided clients in a wide range of industries through several hundred data incidents over the past dozen years. He advises clients on their obligations and helps them operationalize the requirements of General Data Protection Regulation (GDPR) as well as federal and state laws in the U.S. He consults with boards and executive teams on these issues.

Mr. Melodia has been an instructor of Information Security Law in the Chief Information Security Officer (CISO) Executive Education and Certification Program at Carnegie Mellon University's Heinz College, as well as a guest lecturer at Seton Hall Law School and New York University School of Law.

Mr. Melodia served as a law clerk for the Honorable Timothy K. Lewis of the U.S. District Court for the Western District of Pennsylvania.

Experience

Data Security and Privacy Matters

- *Thomas Roger White Jr., et al. v. Sony Electronics Inc., et al.,* Case No. 2:17-cv-01775, in the U.S. District Court for the District of New Jersey. Defending smart TV manufacturer in putative national class action alleging violations of

federal privacy law (VPPA, CFAA, ECPA), New Jersey consumer protection laws, contract law and common law

- *Enslin v. The Coca-Cola Company, et al*., Case No. 2:14-cv-06476-JHS (E.D. Pa.), (granting summary judgment to defendants, denying class certification as moot), reconsideration denied, 2017 WL 3727033 (E.D. Pa. Aug. 29, 2017), aff'd, Nos. 17-3153, 17-3256, 2018 WL 3060098 (3d Cir. June 20, 2018). *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654 (E.D. Pa. 2015) (granting in part motion to dismiss for failure to state a claim). Successfully defended against alleged privacy violations under federal and state law in connection with the theft of 55 laptops containing employee information, including violations of the Driver's Privacy Protection Act (DPPA)
- *Graczyk v. West Publishing Corporation*, 660 F.3d 275 (7th Cir.); *Young v. West Publishing Corporation*, 724 F.Supp. 2d 1268 (2010) (S.D. Fla.); *Johnson v. West Publishing Corporation*, 801 F. Supp. 2d 862 (W.D. Mo. 2011), reversed without opinion by, *Johnson v. West Publishing Corporation*, 504 Fed.Appx. 531 (8th Cir. Apr 09, 2013) (No. 12-1172, 12-1176). Successfully defended West in putative national class actions under the Driver's Privacy Protection Act, obtaining dismissals of all cases
- *Beam v. E-TRADE Financial Corporation*, Case No. CV-2011-64-7 (Ark. Cir. Ct.); *Baxter v. Skype, Inc*., Case No. CV-2011-56-7 (Ark. Cir. Ct); *Baxter v. Philips Electronics North America Corporation*, Case No. CV-201105402 (Ark. Cir. Ct.). October 6, 2011. Secured voluntary dismissals for clients E-TRADE, Skype and PENAC in multimillion-dollar "flash cookie" privacy class actions
- *In Re: Countrywide Financial Corp*. Customer Data Security Breach Litigation, 2012 WL 2873892 (W.D. Ky.). Defended client from more than 40 putative class actions arising from the alleged theft and resale of mortgage-related consumer information; putative national class settlement for class exceeding 17 million persons given final approval; opt out litigation dismissed on our client's motion in *Holmes v. Countrywide Finan. Corp*., 2012 WL 2873892 (W.D. Ky. Jul. 12, 2012)
- *Rowe v. UniCare Life and Health Insurance Company*, Class Action Case No. 09-CV-02286 (N.D.IL). Secured final approval for nationwide class action settlement; in *Rowe*, plaintiffs alleged that the defendant had improperly set data security permissions, resulting in the exposure of healthcare, insurance and payment information for about a quarter-million insureds
- *Saenz v. Kaiser Permanente International*, Case No. 1:09-05562 (N.D. Cal.). Obtained voluntary dismissal for client in putative class action alleging violation of California privacy law resulting in hundreds of alleged identity thefts from a population of approximately 29,000 employees
- *Lockwood v. Certegy Check Services, Inc*., No. 07-CV-01434 (M.D. Fla.). Defended a series of five putative national class actions arising from the theft of consumer information; plaintiffs sought to impose up to $8.5 billion in statutory liability under the Fair Credit Reporting Act (FCRA); proposed favorable settlement given final approval; settlement class includes in excess of 30 million consumers
- *In Re: LendingTree, LLC* Customer Data Security Breach Litigation, MDL 1974 (W.D.N.C.). Obtained two decisions compelling eight putative national class actions to individual (non-class) arbitration
- *Giordano v. Wachovia Securities, LLC and United Parcel Service*, 2006 WL 2177036 (D.N.J. 2006). Established as a matter of first impression the Constitutional point that increased risk of identity theft is not an injury-in-fact and cannot confer federal court subject matter jurisdiction
- *Jurgens v. J.C. Penney Corporation, Inc*., Case No. 12PH-CV00900 (Mo. Cir. Ct.). Negotiated and secured approval of a nationwide class action settlement for J.C. Penney over its use of HTML and Flash Cookies / Local Shared Objects (LSOs).
- *Wood v. Macy's*, Case No. 12PH-CV-00952 (Mo. Cir. Ct.). Negotiated and secured approval of a nationwide class action settlement for Macy's over its use of HTML and Flash Cookies / Local Shared Objects (LSOs).

- *Bell v. Blizzard Entertainment, Inc*., Case No.: 12-CV-09475 (C.D. Cal.). Successfully defended worldwide video game developer and publisher in nationwide class action over its alleged data security practices in relation to an alleged breach
- Obtained dismissal with respect to 31 of 33 claimants on behalf of a major insurance, systems and information technology vendor for the federal government in a multidistrict litigation (MDL) involving eight privacy class actions seeking to impose billions in liability against the company under the FCRA, state consumer protection statutes, and common law theories following the loss of tapes containing protected health information (PHI) and other sensitive personal information on millions of adults and minors

Mortgage and Financial Services Matters

- *U.S. Bank v. Guillaume*, 209 N.J. 449 (N.J. 2012). Represented U.S. Bank, N.A. and obtained a favorable ruling on a challenge to the sufficiency of the pre-foreclosure breach letter; the Court found that pre-foreclosure notice defects are not jurisdictional, overruling a prior appellate decision; the ruling will assist with clearing up the backlog of frozen foreclosure cases in New Jersey
- *Salley v. Option One Mortgage Corp*., 925 A.2d 115 (Pa. 2007). Lead counsel in the Pennsylvania Supreme Court case holding that arbitration agreements in form mortgage contracts are not per se unconscionable because certain creditor remedies are carved out from the requirement to arbitrate; overruling or limiting prior state court decisions
- *Glukowsky v. Equity One*, 848 A.2d 747 (2004), reconsideration denied and certiorari denied 125 S.Ct. 864 (2005). Lead counsel in the New Jersey Supreme Court's preemption-based dismissal of the putative statewide class action challenging the right of state housing creditors to collect prepayment fees from residential mortgage borrowers; the Supreme Court reversed a unanimous appellate panel that had thrown out as *ultra vires* and void an Office of Thrift Supervision (OTS) regulation upon which the mortgage lending industry had long relied; the U.S. Supreme Court denied certiorari, leaving this New Jersey victory intact
- *Gras v. Associates First Capital Corp*., 786 A.2d 886 (N.J. App. Div. 2001). Won, with co-counsel, the then-leading appellate case in New Jersey on the interaction between class actions and mandatory consumer arbitration clauses
- Represented one of the world's largest consumer finance companies in a confidential mediation involving approximately 1,000 mortgage loans to individuals claiming violations of Home Ownership and Equity Protection Act (HOEPA), Real Estate Settlement Procedures Act (RESPA), state fraud laws and federal and state fair lending laws
- *In Re First Franklin Financial Corp*. Litigation, 2010 WL 961649 (N.D. Cal. 2010). Represented multiple national mortgage lenders in class actions alleging racial discrimination, including winning Post-Dukes denial of class certification to potential disparate impact claims *In Re Wells Fargo Residential Mortgage Lending Discrimination Litigation*, 2011 WL 3903117 (N.D. Ca. 2011), and securing approval for national class settlement
- *Alexander v. PSB Lending Corp., et al*., 800 N.E. 2d 984 (Ind. Ct. App. 2003). Obtained early dismissals for one of the largest purchasers of second mortgage loans in the United States from 13 putative class action cases asserting "predatory lending" claims in Colorado, Indiana and New Jersey on the basis that the named plaintiffs all lacked standing to bring suit
- Represented a well-known national consumer lender in Truth in Lending Act (TILA) "mass actions" filed in Florida, North Carolina and California
- Obtained denials of class certification in putative class actions filed against bank clients in Virginia, New Jersey, Maryland and Alabama alleging that the payments of yield spread premiums from lenders to brokers were illegal "kickbacks" under RESPA
- *Beneficial Consumer Discount Company v. Vukman*, 77 A.3d 547 (Pa. 2013). Succeeded in convincing the

Supreme Court of Pennsylvania to review and unanimously reverse a precedential decision of the Superior Court that had held that a form of pre-suit notice used by the entire mortgage industry for more than a decade that failed to include information about credit counseling and loan modification opportunities stripped the trial court of subject matter jurisdiction, thereby throwing into question the finality of final foreclosure judgments in the Commonwealth

- *Horsch et al. v. Wells Fargo*, Case No. 2:14-cv-02638-WY (E.D. Pa). Obtained dismissal of FCRA claims on behalf of Wells Fargo in a putative class action alleging that the bank was not reporting post-bankruptcy payments made to avoid foreclosure and did not add payment details or mark accounts as disputed in response to disputes; remaining claims were resolved on an individual basis
- *In Re Document Irregularities*, No. F-059553-10. Represented mortgage lenders, servicers and trustees in "robo-signing" and other foreclosure-related matters, including Wells Fargo Bank in the New Jersey Order to Show Cause, Docket No. F-9564-12 proceeding

Other Complex and Business Litigation

- *Nuwave Inv. Corp. v. Hyman Beck & Co., Inc*., et al., 2015 WL 2458003,: 114 A.3d 738 (N.J. 2015) Secured unanimous decision by the New Jersey Supreme Court that plaintiff could not reinstate a jury verdict; representing defendant on appeal after three-week jury retrial
- *Treasurer of New Jersey v. AOL Time Warner, et al*., Docket No. MER-L-1349-03. Represented Time Warner and various officers as co-defense counsel in a securities fraud class action arising out of the AOL merger brought on behalf of many of New Jersey's largest state pension funds
- Represented Dell Financial Services in an action brought by New York Attorney General Andrew Cuomo alleging violations of the Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA) as well as of consumer protection laws with respect to financing and sales practices
- *In re Patrick*, No. 5:04–bk–51796–JJT, 2013 WL 951704 (Bkrtcy. M.D. Pa.) (refusing to certify litigation class of debtors against Dell Financial Services). Defended a national consumer class action filed by a putative class of Chapter 13 debtors in the U.S. Bankruptcy Court for the Middle District of Pennsylvania; violations of Sections 506, 1322, and 1325 of the Bankruptcy Code, as well as state law, are alleged; obtained dismissal of all monetary requests for relief, a decision affirmed by the District Court
- *Agostino v. Quest Diagnostic Inc*., 2010 WL 5392688 (D.N.J. 2010) and *Agostino v. Quest Diagnostic Inc.*, 256 F.R.D. 437 (D.N.J. 2009). Represented Quest Diagnostics in putative class action suits alleging improper billing and collection for lab tests
- Defended CIT (as a lease finance company) in class actions and Attorneys General investigations initiated in New York, New Jersey, Illinois, Florida, Texas, California, Massachusetts and elsewhere arising from the collapse of NorVergence
- *Lum v. Bank of America*, 361 F.3d 217 (3d Cir. 2004); 361 F.3d 217, 2004 U.S. LEXIS 4637 (2004), and *Karin J. Black v. JP Morgan Chase, et al*., 2011 WL 4102802 (W.D.Pa.) and 2011 WL 3940236 (W.D.Pa.). Represented one of the nation's largest banks in joint defense efforts that obtained the dismissal of putative class actions alleging antitrust and Racketeer Influenced and Corrupt Organizations Act (RICO) conspiracies to fix the prime rate and to fix credit prices and availability using Fair Isaac Corporation (FICO) and other credit scoring systems
- *In Re New Valley*, 181 F.3d 517 (3rd Cir. 1999). Won approximately $3 million after a three-week trial in bankruptcy court on behalf of a commercial landlord and sustained that judgment on appeal before the Court of Appeals for the Third Circuit
- *Safeco Life Ins. Co. v. Singer Asset Fin. Co*., No. C99-1626 (W.D. Wash. March 9, 2000), advantageously settling a

national class action (See, *Waldeier v. J.G. Wentworth S.S.C. Ltd.*, No. 4064 (P.C.C.P. May 24, 2001)), and representing the industry as amicus in the New Jersey Supreme Court. (*Owen v. CNA Insurance Company, et al*., 771 A.2d 1208 (2000)). Coordinated and implemented a national defense strategy for the industry which created a secondary market by purchasing structured settlement payment streams

- *Trump v. O'Brien* _29 A.3d 1090, 2011 WL 3903013 (N.J. App. Div. 2011) and *Trump v. O'Brien,* 403 N.J. Super. 281, 958 A.2d 85 (N.J. App. Div. 2008). As co-defense counsel, protected confidential sources under the newsperson's privilege and ultimately won summary judgment for the former Warner Books and one of its authors in a defamation case brought by Donald J. Trump in connection with the publication of "Trump Nation"

Credentials

Education

- New York University School of Law, J.D., *cum laude*
- Princeton University, Woodrow Wilson School of Public and International Affairs, A.B., *cum laude*

Bar Admissions/Licenses

- New Jersey
- New York
- Pennsylvania

Court Admissions

- U.S. Supreme Court
- U.S. Court of Appeals for the Third Circuit
- U.S. Court of Appeals for the Fourth Circuit
- U.S. Court of Appeals for the Sixth Circuit
- U.S. Court of Appeals for the Seventh Circuit
- U.S. Court of Appeals for the Eighth Circuit
- U.S. Court of Appeals for the Eleventh Circuit
- U.S. District Court for the Eastern District of New York
- U.S. District Court for the Northern District of New York
- U.S. District Court for the Southern District of New York
- U.S. District Court for the District of New Jersey
- U.S. District Court for the Eastern District of Pennsylvania
- U.S. District Court for the Western District of Pennsylvania
- U.S. District Court for the Middle District of Pennsylvania

Memberships

- The American Law Institute, Elected Member, 2012
- *Law360* Privacy & Consumer Protection, Advisory Board, 2012-2017
- American Bar Association

- Bar Association of the Third Federal Circuit
- New York Bar Association

Honors & Awards

- *Chambers Global – The World's Leading Lawyers for Business* guide, Privacy & Data Security: Litigation, 2020
- *Chambers USA – America's Leading Business Lawyers* guide, Privacy & Data Security: Litigation, 2019, 2020
- *National Law Journal*, Cybersecurity & Data Privacy Trailblazer, 2015
- *Law 360,* MVP in Privacy & Consumer Protection, 2011
- New Jersey *Super Lawyers* magazine, Class Action and Mass Torts, 2005-2006, 2014-2015, 2017-2018
- *NJ Biz*, 40-Under-40, New Jersey's Most Successful Business People, 2003
- The Order of Barristers, National Member
- New York University School of Law Moot Court Board, Competitions Director; Executive Committee

Publications

- 10 Practical Tips for Employers to Safeguard Their Trade Secrets During COVID-19, *Holland & Knight Trade Secrets Blog*, April 20, 2020
- A Report on Businesses' Implementation of the California Consumer Privacy Act in the First Month, February 12, 2020
- Holland & Knight's Israel Practice Newsletter: Fall-Winter 2019, December 17, 2019
- Cybersecurity Checklist : 12 Security Risks Hotels Must Address, Author, *Hotel Business Review*, December 8, 2019
- California Attorney General Releases Draft Regulations on the California Consumer Privacy Act, *Holland & Knight Alert*, October 31, 2019
- Hospitality Industry Prepares for Slate of New Consumer Privacy Protections, *Holland & Knight Alert*, October 7, 2019
- Harbinger or Outlier? Is 'Dittman' Creating a New Common Law Privacy Obligation on Employers?, *New York Law Journal*, March 7, 2019
- Bracing for the Big One: The Impact of the California Consumer Privacy Act on E-Discovery, *New York Law Journal*, February 1, 2019
- Patchy State Regulation Raises Questions for Drone Use, Co-Author, *The Legal Intelligencer*, June 23, 2016
- Making Informed Choices About the Deep, Dark Web, Co-Author, *Law.com*, June 3, 2016
- Legal Risk and Rules of the Move to Biometrics, Co-Author, *New York Law Journal*, March 2, 2015
- Is Your Franchise System Prepared for a Cyber Attack?, Co-Author, *Franchise Times*, May 2014

Speaking Engagements

- Data Privacy & Security Trends, Data Hostage Negotiations, & Cybercrime, Speaker, Florida Bar Annual Convention, June 19, 2020
- Financial Services Technology 2020: Avoidance of Risk, Practising Law Institute, April 7, 2020

- SEC Regulation of Public Companies and Law Firms in the Context of Cybersecurity, Panelist, SEC Regulation of Public Companies and Law Firms in the Context of Cyber Security, Cybersecurity Best Practices for Legal Services Providers 2020, February 3, 2020
- GDPR: The State of Readiness 18 Months Later, Panelist, European American Chamber of Commerce, New York Chapter, December 3, 2019
- Ethical Issues in Emerging Technologies for In-house Counsel, Speaker, Retail Industry Leaders Association Retail Law Conference 2019, October 16-18, 2019
- Mortgage Bankers Association Legal Issues and Regulatory Compliance Conference, Panelist, Fintech/Regtech Track: Data Security and Privacy Update, May 5-8, 2019
- Data Security Issues Facing Financial Institutions – a CISO's Perspective, Panelist, Financial Services Technology 2019: Avoidance of Risk, April 25, 2019
- Cybersecurity Best Practices for Legal Services Providers 2019, Panelist, SEC Regulation of Public Companies and Law Firms in the Context of Cyber Security, Practising Law Institute, February 4, 2019
- Privacy and the Internet of Things (IoT), Panelist, New York State Bar Association Intellectual Property Law Section Annual Meeting, January 15, 2019
- Exploring the New Normal In Consumer Protection Enforcement, Holland & Knight and NBA-CLS Event, November 16, 2018
- Data Privacy & Security: Legal Landscape, Pittsburgh ISACA's Annual Security Conference, December 5, 2016
- Class Action Liability and The Internet of Things, The Union League of Philadelphia Seminar, September 17, 2015
- Data Security and Data Privacy, GAMA Policy and Legal Issues Committee Meeting, July 28, 2015
- Privacy and Data Security: Oh No … I've Been Hacked!, Entertainment Industry Conference, June 5, 2015
- Cybersecurity and Data Breach: The New Reality for Directors and Those Who Advise Them, 35th Annual Ray Garrett Jr. Corporate and Securities law Institute Seminar, April 30-May 1, 2015
- Protecting Brands in the Event of a Data Breach, Association of National Advertisers Webinar, September 16, 2014
- The Risk-Based Approach to Data Breach Response, International Association of Privacy Professionals (IAPP) Global Privacy Summit, March 6, 2014
- Data Protection and Privacy in Franchising: Who is Responsible?, American Bar Association 36th Annual Forum on Franchising, October 17, 2013
- Dealing with Cybersecurity Issues, Institute of International Bankers Annual Risk Management and Regulatory Examination/Compliance Seminar, October 8, 2013
- Private and Government-Related Consumer Litigation, Federal Bar Association Annual Meeting, September 26, 2013

Holland & Knight

Ashley L. Shively

PARTNER

Ashley.Shively@hklaw.com

San Francisco
415.743.6906

PRACTICES
Litigation and Dispute Resolution | Financial Services Litigation | Financial Services | Financial Services Regulations | Technology | Class Action Litigation and Arbitration | Consumer Protection Defense and Compliance | Data Strategy, Security & Privacy | TCPA Class Action Litigation

INDUSTRY
Technology & Telecommunications

Ashley L. Shively is a privacy attorney and class action litigator in Holland & Knight's San Francisco office.

Ms. Shively counsels public and privacy companies on consumer protection and data privacy issues with respect to product development, sign-up and point-of-sale procedures, digital marketing, regulatory compliance, and state and federal enforcement. She regularly advises on the Children's Online Privacy Protection Act (COPPA), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), state privacy and unfair and deceptive practices laws, and similar legal and regulatory requirements. At present, she is particularly focused on the California Consumer Privacy Act (CCPA), and writes and speaks frequently on the topic.

Ms. Shively focuses her litigation practice on the defense of financial institutions and businesses in consumer class and individual actions, including privacy, data breach, false advertising, unfair business practices, fair lending, credit reporting and debt collection. She has extensive experience litigating class actions under the Truth in Lending Act (TILA), Telephone Consumer Protection Act (TCPA) and California's Invasion of Privacy Act (CIPA).

Ms. Shively also handles complex litigation matters, from mass tort and federal multidistrict litigation to commercial contract disputes. She represents public agencies and private businesses affected by litigation brought under the California Public Records Act, and clients in matters involving the FCC and other regulatory agencies.

Immediately after law school, Ms. Shively worked in the complex and civil divisions of the Superior Court of California of the County of Alameda. She also externed during law school for the Honorable Frank C. Damrell in the U.S. District Court for the Eastern District of California and the Honorable Robert L. Dondero in the Superior Court of California of the County of San Francisco.

Experience

Representative Counseling Matters

- Advise clients on the adoption and implementation of data privacy program in light of evolving laws and regulations,

including the California Consumer Privacy Act (CCPA), European Union General Data Protection Regulation (GDPR)

- Advise FinTechs on call center and text message scripting for compliance with state call recording laws and the Telephone Consumer Protection Act (TCPA)
- Advise financial institution and retail company on third-party risk management and services agreements
- Advise on privacy policies, customer terms and conditions, and other consumer-facing policies and internal data privacy procedures
- Counsel businesses across industry sectors on compliance with consumer privacy statutes, including California's Shine the Light Act and Automatic Renewal Law, and the Illinois Biometric Information Privacy Act (BIPA), and state and federal consumer protection obligations

Representative Litigation Matters

- Represented a FinTech client in investigation by enforcement division of federal regulator on consumer protection issues
- Defended pharmaceutical division of foreign entity in antitrust class action and secured dismissal with prejudice of key claims at the pleading stage (U.S. District Court for the Northern District of California)
- Secured dismissal with prejudice on first round of motion practice in a Telephone Consumer Protection Act (TCPA) class action filed against technology company (U.S. District Court for the Northern District of California)
- Represented a private educational institution in series of nationwide putative class actions alleging violations of various consumer protection statutes (U.S. District Court for the Central District of California)
- Secured a seven-figure reduction in attorneys' fee award on litigated fee motion in connection with settlement of certified nationwide class (U.S. District Court for the Northern District of California)
- Defeated class certification on behalf of financial institution in a TCPA action (U.S. District Court for the Northern District of California)
- Defended a student loan servicer in putative class action alleging call recordings in violation of California's Invasion of Privacy Act (U.S. District Court for the Northern District of California)
- Defeated class certification and obtained summary judgment on behalf of an auto-finance company in coordinated TCPA class actions (U.S. District Court for the Northern District of Illinois)
- Represented a music streaming service in false advertising class action and negotiated favorable individual settlement (U.S. District Court for the Southern District of New York)
- Represented a healthcare provider in a data breach class action under California's Customer Records Act and Confidentiality of Medical Information Act (Superior Court of California, Contra Costa County)
- Negotiated a favorable class settlement on behalf of an auto-finance company for alleged violations of California's Rees-Levering Act related to post-repossession notices (Superior Court of California, Contra Costa County)
- Defense of mandate lawsuits and response in three appellate proceedings arising from rulings / judgments in favor of state agency in facilities dispute, followed by settlement that yielded multiyear facilities agreement (Superior Court of California, Santa Clara County)
- Defended a beverage company in right of publicity action (Superior Court of California, San Diego County)
- Represented a technology platform in dispute with advertising agency and digital publishers over click fraud, malware and other forms of ad fraud (Superior Court of California, San Francisco County)
- Defended a cosmetics company in a putative class action alleging violations of California's Song-Beverly Consumer

Warranty Act related to ZIP code recording at point-of-sale and secured approval of class settlement (Superior Court of California, San Francisco County)

- Seminal published opinion affirming right of state agency to maintain privacy of unpublished researchers' files (Superior Court of California, Yolo County and Court of Appeals of California, Third District)
- Defended a state agency in mandamus action filed by Public Records Act requestor related to unpublished researched files and sensitive identifying information (Superior Court of California, Yolo County)

Credentials

Education

- University of California Davis School of Law, J.D.
- The Johns Hopkins University, M.A., Government
- The Johns Hopkins University, B.A.

Bar Admissions/Licenses

- California

Court Admissions

- U.S. Court of Appeals for the Ninth Circuit
- U.S. District Court for the Northern District of California
- U.S. District Court for the Central District of California
- U.S. District Court for the Eastern District of California
- U.S. District Court for the Southern District of California
- U.S. District Court for the Northern District of Illinois

Memberships

- Association of Business Trial Lawyers (ABTL), Leadership Development Committee
- American Bar Association
- The Bar Association of San Francisco

Honors & Awards

- Holland & Knight Rising Star, Class of 2020

Publications

- A Report on Businesses' Implementation of the California Consumer Privacy Act in the First Month, February 12, 2020
- Holland & Knight's Israel Practice Newsletter: Fall-Winter 2019, December 17, 2019
- California Attorney General Releases Draft Regulations on the California Consumer Privacy Act, *Holland & Knight Alert*, October 31, 2019
- Hospitality Industry Prepares for Slate of New Consumer Privacy Protections, *Holland & Knight Alert*, October 7,

2019

- California Consumer Privacy Act Amendments Head to Gov. Newsom's Desk, *Holland & Knight Alert*, September 20, 2019
- Holland & Knight's China Practice Newsletter: July-August 2019, *Holland & Knight Newsletter*, July-August 2019
- California Consumer Privacy Act Update: Assembly Approves 12 Amendments, *Holland & Knight Alert*, June 6, 2019
- Holland & Knight's China Practice Newsletter: May-June 2019, Class Actions: A Uniquely American Litigation Tool, *Holland & Knight Newsletter*, May-June 2019
- Washington State Pushes Forward With Comprehensive Privacy Legislation, *Holland & Knight Privacy Blog*, March 27, 2019
- Final Public Forum Held on California Consumer Privacy Act, *Holland & Knight Alert*, March 7, 2019
- When Worlds Collide – Navigating Fintech/Traditional Bank Partnerships to Deliver Value to Consumers, *Bloomberg*, April 2, 2018

Speaking Engagements

- Managing Legal Risks in Online Business Activities, Holland & Knight Webinar, May 4, 2020
- Seismic Shifts in the Privacy Landscape, Moderator, 33rd Annual Corporate Counsel Conference, The Commercial Law Section, National Bar Association, February 14-15, 2020
- The Wild West of Law Firm Cybersecurity & Privacy: The What, Why, How and Ethics of Protecting Client Data , Panelist, 5th Annual MCLE Spectacular Seminar, Contra Costa Bar Association Business Law Section, November 22, 2019
- Firm General Counsel Summit, September 25-27, 2019
- Advanced In-House Counsel, Cybersecurity and Data Privacy: The Evolving Legal Landscape and Landmines, TexasBarCLE, August 8-9, 2019

Holland & Knight

Anthony J. Palermo

ASSOCIATE

Anthony.Palermo@hklaw.com

Tampa
813.227.6320

PRACTICES
Litigation and Dispute Resolution | Regulatory and Federal Litigation | Consumer Protection Defense and Compliance | Financial Services | Financial Services Litigation | Financial Services Regulations | Data Strategy, Security & Privacy | TCPA Class Action Litigation

INDUSTRIES
Healthcare & Life Sciences | Transportation & Infrastructure | Technology & Telecommunications

Anthony J. Palermo is a Tampa litigation attorney who represents clients in complex commercial disputes, governmental investigations, enforcement actions, and administrative proceedings, arbitrations, and state and federal court litigation, including through trial and appeal. Mr. Palermo also advises clients on regulatory compliance and corporate governance issues with a particular focus on consumer protection and financial services laws and regulations. He has significant experience in the financial services, transportation, healthcare, and telecommunications industries.

Mr. Palermo has been recognized as one of the top lawyers in Tampa for commercial litigation as well as banking and finance litigation by *Tampa Magazine*, one of the "Rising Stars" in the state of Florida by *Super Lawyers*, and as a "Florida Legal Elite" attorney for commercial litigation by *Florida Trend* magazine. In addition, he was previously recognized nationally as one of only five consumer protection attorneys to be honored as a *Law360* Rising Star and named to its list of top attorneys "whose legal accomplishments transcend their age."

As part of his litigation practice, Mr. Palermo has represented multiple professional sports teams in Florida, including Major League Baseball and National Hockey League franchises. As part of his regulatory practice, Mr. Palermo has been appointed a Special Assistant Attorney General to advise a state-run lending institution on compliance with consumer protection and banking laws.

In addition, Mr. Palermo has held various positions of bar leadership and is the chair of The Florida Bar's Consumer Protection Law Committee. He is a frequent speaker at continuing legal education courses for The Florida Bar and has authored articles for multiple legal publications. His published work has been quoted in law review articles, cited as support in appellate briefs by other lawyers before courts throughout Florida, and cited with approval in a recent decision by Florida's Second District Court of Appeal, which has appellate jurisdiction over the state courts in Hillsborough County, Florida, including Tampa.

Mr. Palermo's recent representative matters include:

- defended Florida-based international company, employee, and director in federal court and U.S. Court of Appeals for the Fourth Circuit; obtained final judgment in defendants' favor and prevailed in appeal after defeating claims of

fraud, misrepresentation, and violations of Unfair and Deceptive Trade Practices Act (UDTPA) and Racketeer Influenced and Corrupt Organizations Act (RICO)

- represented a Major League Baseball (MLB) franchise in multiyear litigation subject to local and national media coverage
- represented an operator of a professional sports arena in a breach of contract action in federal court
- represented a National Hockey League (NHL) franchise in a trademark infringement dispute
- defended a surgery center in federal court against a putative class action arising from a data breach involving an alleged 142,000 patients; obtained an order dismissing all claims regarding a "novel" issue of law for which "circuit courts have reached conflicting conclusions" and that had "not been addressed by the Eleventh Circuit"
- prosecuted a breach of contract action on behalf of a business broker; obtained dismissal of counterclaims for fraud in the inducement and rescission, and obtained an order compelling the production of key discovery and subject of the claim for breach and awarding attorneys' fees and costs
- defended a financial services corporation against a putative class action based on alleged violations of the Florida Consumer Collection Practices Act (FCCPA) and Fair Debt Collection Practices Act (FDCPA); resolved on an individual basis with the plaintiff after filing a dispositive motion
- defended a debt-buying company and account-servicing corporation in seven different lawsuits filed by multiple plaintiffs in Florida state court and defeated claims of alleged FCCPA and FDCPA violations after removing to federal court, consolidating cases, and prevailing on a motion for summary judgment and obtaining an order granting final judgment in the defendants' favor
- represented a national bank in a three-day trial; obtained final judgment declaring that the client had a top priority security interest in the collateral
- prosecuted an action on behalf of a transportation and logistics company for breach of option contract and conversion; obtained order striking opposing party's responsive pleading
- defended a real estate development company against claims of alleged business torts and breach of contract; obtained dismissal with prejudice of multiple claims, including for civil theft

While attending law school, Mr. Palermo was a teaching fellow at Harvard in the government department and received the Harvard University Certificate of Distinction in Teaching. Prior to law school, Mr. Palermo worked for the National Geospatial-Intelligence Agency, a combat support agency for the U.S. Department of Defense, where he held Top Secret/SCI level security clearance and traveled internationally as part of a U.S. delegation to the Global Dialogues on Emerging Science and Technology conference in Cape Town, South Africa.

Experience

Banking and Financial Services Litigation

- Represented a national bank in a three-day trial in an action for a breach of loan agreement, breach of promissory note, and breach of guaranty; obtained final judgment declaring that the client had a top priority security interest in fees payable to the borrower
- Defended former officers and directors of multiple community banks in three separate actions filed by the Federal Deposit Insurance Corp. (FDIC) for claims of alleged negligence, gross negligence, and breach of fiduciary duty
- Represented a business broker and a mergers and acquisitions (M&A) advisory firm in multistate litigation; obtained a publicly filed stipulation from the opposing party admitting contract was valid and enforceable, acknowledging liability under the contract, and withdrawing all prior allegations against the client

- Defended a bank against claims of breach of contract, fraud in the inducement, misleading advertisement, and negligent misrepresentation; obtained an order striking the claim for punitive damages and awarding attorneys' fees
- Defended multiple insurance companies against claims of tortious interference and unjust enrichment in a putative class action in a Florida state court; obtained order granting motion for sanctions and dismissal with prejudice

Probate Litigation

- Obtained final judgment in favor of individual clients in probate litigation after full evidentiary hearing

Healthcare Litigation

- Defended a surgery center against a putative class action; obtained dismissal of multiple claims and denial of motion for class certification in order where the federal court found "there is no clear consensus as to how the issue should be resolved," but "[c]onsidering the arguments on both sides, the Court agrees with [defendant]" as to "novel" issue of "whether a data breach on its own is an 'injury in fact'" and, therefore, "[t]he Court concludes the action should be dismissed" and plaintiffs "lack standing to sue"
- Defended a healthcare facility during a binding, two-day arbitration regarding a joint venture buyout dispute with a minority owner that implicated Stark Law and Anti-Kickback Statute; argued evidentiary issues and cross-examined opposing expert witness
- Obtained temporary injunction, then a permanent injunction and final judgment in favor of an assisted-living facility, allowing the facility to terminate a contract after full evidentiary hearing

Public Contracts and Public Finance Litigation

- Represented a client selected for an award of public contract in its response to request for a proposal and the ensuing evaluation process by the Hillsborough County Aviation Authority
- Represented a government-control district and body corporate of the State of Florida in a bond validation action; obtained final judgment that found the financing at issue was valid, legal, and binding, which validated and confirmed related proceedings by district

Corporate Compliance and Regulatory Guidance

- Appointed Special Assistant Attorney General and advised the state-run housing and lending authority regarding compliance with rules implemented by the Consumer Financial Protection Bureau (CFPB) under the Dodd-Frank Act and regulations enacted under the Truth in Lending Act (TILA) and Real Estate Settlement Procedures Act (RESPA)
- Advising a multinational pharmaceutical and medical-device company regarding compliance with the Telephone Consumer Protection Act (TCPA) and negotiated healthcare-related product delivery arrangements with multiple different companies on the client's behalf to reduce risk based on structuring agreement to qualify for relevant safe harbors and exceptions pursuant to regulations and orders of the Federal Trade Commission (FTC) and Federal Communications Commission (FCC)
- Advised a publicly traded retailer regarding regulatory compliance risks regarding the acquisition of a financial services company
- Advising one of the largest healthcare clinics in the Southeastern United States regarding compliance with various consumer protection laws and assisting with patient intake forms, privacy policies, and financial agreements
- Advising a multistate supermarket chain and pharmacy regarding compliance with TCPA and other privacy and

consumer-related laws and regulations, as well as providing guidance for developing content of customer communications and messaging, preparing consent forms, and online and app-based terms of use and privacy policies

Governmental Investigations, Regulatory Examinations, and Administrative Proceedings

- Defended a leading company in the hospitality industry in an investigation by the CFPB, resulting in the government's closing of its investigation, withdrawal of its civil investigative demand and document-retention obligations, and a decision not to take enforcement action
- Represented a regional bank in Florida under examination by the Office of the Comptroller of the Currency (OCC) after the OCC questioned whether the bank's lending practices for foreign nationals complied with the Equal Credit Opportunity Act (ECOA); submitted an analysis of the practices in question resulting in the OCC concluding that the bank's practices did not present any fair lending issues
- Represented a storage corporation in an administrative appeal of a stop-work order and order of penalty assessment based on alleged violations of workers' compensation laws; obtained order significantly reducing assessed penalty
- Represented a construction company in an administrative appeal of a stop-work order and order of penalty assessment based on alleged violations of workers' compensation laws; obtained an order significantly reducing assessed penalty

Transportation Litigation

- Defended a hauling company and obtained an order denying a claim for punitive damages after multiple evidentiary hearings based upon, among other things, compliance with the U.S. Department of Transportation (DOT) standards, despite the court allowing the claim of punitive damages to proceed against the driver after the trucking accident
- Represented multiple transportation and logistics companies in various disputes related to noncompetition, nondisclosure, and nonsolicitation provisions in agreements with subcontractors
- Represented a transportation and logistics company in an indemnity action against a sub-hauler stemming from a prior personal injury action
- Represented a transportation and logistics company in a dispute with a former customer arising from a multiyear business relationship governed by tariffs and multiple contractual arrangements
- Defended a transportation and logistics company in a dispute with a shipping agency regarding invoices arising under an intermodal interchange and facilities access agreement

Telecommunications Litigation

- Represented a telecommunications company in an adversary proceeding in bankruptcy court in a constructive fraudulent transfer action
- Represented a telecommunications company in a tax controversy and obtained summary judgment defeating the IRS' claim of a superior creditor interest in the client's real property
- Represented a telecommunications company in a multimillion-dollar, international dispute relating to multiple breach of contract claims and business torts
- Representing a leading global mobile and network communications company in an international contractual dispute with a national public telecommunications company operated by a foreign government

Pro Bono Service for Hurricane Survivors

- Received the President's Award from The Young Lawyers Division of The Florida Bar for pro bono services related to natural disasters in 2018 and 2019
  - In June 2019, he earned the honor for "outstanding service to the young lawyers of Florida and his contributions to the betterment of the legal profession" for similar pro bono service in the wake of Hurricane Michael.
  - In June 2018, received the recognition for distinguished leadership, service and contributions to the legal profession for coordinating a statewide response to Hurricane Irma between the Federal Emergency Management Agency (FEMA), the American Bar Association (ABA), The Florida Bar, and legal aid providers and volunteer attorneys. As a result, more than 460 attorney volunteers provided free legal assistance to over 2,000 Floridians who could not afford to retain an attorney to address legal issues resulting from the storm.

Credentials

Education

- Harvard Law School, J.D.
- The University of North Carolina at Chapel Hill, B.A., Political Science, minor in Philosophy, *with highest distinction*

Bar Admissions/Licenses

- Florida

Court Admissions

- U.S. District Court for the Middle District of Florida
- U.S. District Court for the Northern District of Florida
- U.S. Bankruptcy Court for the Middle District of Florida
- U.S. District Court for the Southern District of Florida
- U.S. Court of Appeals for the Fourth Circuit

Memberships

- The Florida Bar, Consumer Protection Law Committee, Chair, 2020-Present; Vice Chair, 2019-2020; CLE Subcommittee Chair, 2018-2019; Appointed Member, 2016-Present
- The Florida Bar Young Lawyers Division (YLD), Board of Governors, 2017-2019
- American Bar Association Young Lawyers Division (YLD), District Representative for Florida, 2017-2019; Corporate Counsel Committee, Co-Chair, 2017-2019; Vice Chair 2015-2017; Litigation Committee, Vice Chair, 2014-2015
- The Florida Bar, Leadership Academy, Fellow, 2015-2016
- Hillsborough County Bar Association, Leadership Institute, Chair, 2014-2015
- Tampa Bay Carolina Club, President, 2016-2019
- Harvard College, Admissions Office, Interviewer
- Harvard Club of Tampa Bay, President, 2015-2017
- Best Buddies Tampa Bay, Advisory Board, 2012-2014
- Tampa Hispanic Bar Association

Holland & Knight

Honors & Awards

- Florida Legal Elite, *Florida Trend* magazine, 2020
- Top Lawyer, Litigation: Banking & Finance, *Tampa Magazine*, 2020
- Top Lawyer, Commercial Litigation & Transactions Law, *Tampa Magazine*, 2017-2018
- Rising Star, Consumer Protection, *Law360,* 2018
- President's Award, The Florida Bar YLD, 2018-2019
- Rising Star, Florida *Super Lawyers* magazine, 2015-2020
- Up & Comer, Florida Legal Elite, *Florida Trend* magazine, 2016-2019
- Star of the Quarter, American Bar Association YLD, Fall 2017
- Public and Charitable Service All-Star, Holland & Knight, 2018; Pro Bono All-Star, 2017-2019
- Proven Pro Bono Producer Award, Hillsborough County Bar Association, 2016-2020
- ABA Military Pro Bono Project Outstanding Services Award, 2018
- Up & Comer, Under 30 Category, *Tampa Bay Business Journal*, 2015
- Certificate of Distinction in Teaching, Harvard University
- Order of the Bell Tower, University of North Carolina at Chapel Hill

Publications

- Lessons Learned in Providing Disaster Legal Services in Florida, *ABA Law Practice Today*, December 2017
- The Parental Leave Rule: A Procedural Rule for Effecting Change, *Corporate Counsel ABA Young Lawyers Division Newsletter*, Fall 2017
- Watch Your Standing: Don't Trip on a Litigation "Oddity", Hillsborough County Bar Association, Vol. 28, No. 1, *Lawyer Magazine*, September 7, 2017
- 4 Things To Remember About Refill Reminder Compliance, *Law360*, July 13, 2017
- A Prescription for Complying with the TCPA's Proscriptions: *Zani v. Rite Aid Headquarters Corp.* , *Holland & Knight Publication*, July 6, 2017
- How To Respond When CFPB Comes Knocking, *Law360*, October 5, 2016
- Highlights from Seminar on Governmental Investigations Involving the Debt Collection Industry, *Holland & Knight Alert*, September 14, 2016
- Attention Lenders! The TILA-RESPA Integrated Disclosure Rule Is Taking Effect: Two New Disclosure Forms Are Required for Most Closed-End Consumer Mortgage Loans, *Corporate Counsel ABA Young Lawyers Division Newsletter*, Fall 2015
- Doctors as Debt Collectors? Healthcare Providers and the Florida Consumer Collection Practices Act, *Florida Law Review Forum*, Volume 67, September 2015

Speaking Engagements

- Data Privacy & Security Trends, Data Hostage Negotiations, & Cybercrime, Moderator, Florida Bar Annual Convention, June 19, 2020
- Disaster Law – Legal Issues and Coordinating with FEMA in Wake of Natural Disaster, Guest Lecturer, Stetson

University College of Law, February 9, 2020

- Protecting Consumers Who Have Unconventional Needs with Conventional Strategies: Making Florida Safe for Military and Elderly Consumers, Co-Presenter, The Florida Bar Consumer Protection Law Committee and the Elder Law Section, June 29, 2019
- Depositions, The Florida Bar Basic Discovery CLE, April 25, 2019
- Lending and Leasing to Servicemembers, Holland & Knight Webinar, April 4, 2019
- Practicing with Professionalism, The Florida Bar Continuing Legal Education Committee and YLD, March 29, 2019
- Providing Pro Bono Assistance to Survivors of A Natural Disaster, ABA Consumer Financial Services Committee Meeting, January 10-13, 2019
- Insights and Perspective on Navigating Between In-House and Outside Counsel, ABA YLD Corporate Counsel Committee and Labor & Employment Committee, August 1, 2018
- Let's Work Together: Meeting a Corporate Client’s Goals in a Representation, Moderator, ABA YLD Corporate Counsel and Litigation Committees Teleconference, July 25, 2018
- Doing Well While Doing Good: Public-Private Partnerships, Moderator, Florida Bar Consumer Protection Law Committee CLE, June 15, 2018
- Hot Topics in Corporate Law: The Telephone Consumer Protection Act, ABA YLD Corporate Counsel Committee Teleconference, February 28, 2018
- Business Torts and Remedies, The Florida Bar Basic Business Litigation 2018, February 23, 2018
- Practicing with Professionalism, The Florida Bar Continuing Legal Education Committee and YLD, August 4, 2017
- You’ve Heard from the CFPB and FTC: Now What?, Holland & Knight Webinar, October 19, 2016
- Basic Consumer Protection Law, The Florida Bar's Basic Business Law 2016, May 20, 2016
- You've Got the Right Stuff, Baby: What Corporate Counsel Look for in Outside Counsel, ABA YLD Corporate Counsel Committee Teleconference, Panelist, March 7, 2016
- Law Firm Management, ABA YLD Litigation Committee Teleconference, Moderator, January 27, 2015
- Careers in Criminal Law, ABA YLD Litigation Committee Teleconference, Moderator, November 14, 2014
- Practicing with Professionalism, The Florida Bar Continuing Legal Education Committee and YLD, Panelist, September 11, 2014