ACC Association of Corporate Counsel
GREATER PHILADELPHIA

PRIVACY AND THE EVOLVING LITIGATION AND COMPLIANCE LANDSCAPE

Panelists:

Deb Carlos – Vice President and Deputy General Counsel, Comcast
Kate Deal – Partner, Akin Gump Strauss Hauer & Feld LLP
Kate Katchen – Partner, Akin Gump Strauss Hauer & Feld LLP
Meredith Slawe – Partner, Akin Gump Strauss Hauer & Feld LLP

Follow us on social media!

@accgp **@delvacca**

April 24, 2019 In-House Counsel Conference:
General Counsel/Chief Legal Officer Track

Overview

- Some of the most significant class action and individual lawsuits filed in federal and state courts across the country involve consumer, employee and patient privacy issues.
- Cutting-edge technology offers businesses unprecedented access to valuable data, including personal identifying information, while creating a host of compliance challenges.
- The privacy litigation landscape is complicated by a patchwork of existing state and federal laws and emerging new laws that are driven by coordinated lobbying efforts and state AGs with political ambitions.
- Compliance is key. And privilege attached to compliance audits/efforts is critically important.
- It can be difficult to ascertain what issues are truly worthy of concern and require risk mitigation strategies, and where there is unnecessary alarm.

Overview

Privacy litigation environment in the U.S. in the age of GDPR and stricter regimes in the EU and abroad (a game of “catch up”).

Demystify the privacy class action landscape.

- Noting areas of heightened risk – where companies have presence/customers in California, Illinois or internationally.
- Identifying key players in the plaintiffs’ class action bar (and what captures their attention and deters them from filing suit).
- Discussing the reality of the privacy class action – effort to leverage aggregate damages, disruption to the business, defense costs, burdens of discovery → to extract large settlements.

Unique privacy issues related to opioid litigation.

- Protected substance abuse treatment information.
- Government and private-plaintiff challenges to pharma opioid data and documents.

Key statutes that are part of the wave of privacy-based litigation

Telephone Consumer Protection Act (TCPA)
(federal)

Biometric Information Privacy Act (BIPA)
(Illinois) and its counterparts (Washington; Texas – government enforcement only)

Invasion of Privacy Act (CIPA)
(California)

Wiretap Act
(federal)

Shine the Light Law (STLL)
(California)

Fair Credit Reporting Act (FCRA)
(federal)

Children's Online Privacy Protection Act (COPPA)
(federal)

Video Privacy Protection Act (VPPA)
(federal)

Song-Beverly Credit Card Act
(California) and its counterpart (Massachusetts)

Public Health Service Act
(federal)

42 C.F.R. Part 2

The topic that every company doing business in California is thinking about

The California Consumer Privacy Act (CCPA)

(effective January 2020)

- Far-reaching law that redefines what constitutes “personal information.”
- Misinformation about the breadth and scope of its private right of action.
- Spirit of this law has some of the core principles written in GDPR.
- Will CCPA prompt a sweeping federal data privacy law?

Today’s agenda

- TCPA
- BIPA
- CCPA
- Health Care Privacy

Ways to mitigate class action risk

- Privacy audits (privileged!)
- Robust and carefully-crafted policies
- Compliant practices
  (with any issues being depicted as isolated, individualized transgressions)
- Active vendor management
- Indemnification and insurance
- Arbitration agreements with class action waivers interposed in consumer-facing terms

Practical Tips

- click-wrap/browse-wrap
- evidence of formation
- broadly crafted
- scope for arbitrator to decide
- failing to include consumer friendly provisions

New tech tools offer companies access to rich consumer data

"AI will probably most likely lead to the end of the world, but in the meantime, there'll be great companies."

– **Sam Altman**
Chairman, Y Combinator; Co-Chairman of OpenAI

How You Can Use Location Tracking Features in Mobile Apps to Create Targeted Advertising Experiences

Eyes on the Road! (Your Car Is Watching)

Facial recognition scanning goes mainstream

How Machine Learning, Wearables and Smart Devices Could Close the Skills Gap Once and For All

California startup predicts retail failure via satellite images

Can airplane seat cameras spy on passengers?

The Revolution of Artificial Intelligence

Using Machine Learning To Improve Restaurant Management

Best Practices for Supply Chain Cybersecurity

Artificial Intelligence Can Now Write Amazing Content – – What Does That Mean For Humans?

Identify Threats and Prevent Crime

A Complete Facial Recognition Platform that is Accurate, Scalable, Private and Secure

Life Insurers Can Use Social Media Data in Underwriting. Should They?

When it comes to social media manipulation, we're our own worst enemy

WHAT IS THE WORKING OF IMAGE RECOGNITION AND HOW IT IS USED?

A Retail Dilemma: Consumers Believe In Pictures As Digital Trust Declines

Drug Developers Circumspect About Using Social Media in Clinical Research, According to the Tufts Center for the Study of Drug Development

Personalized Health Care and Artificial Intelligence Could Improve Your Life—at the Cost of Your Privacy

Tech & insurance: How wearable gadgets could rule the future of healthcare

Cloud Vision

What are the Legal and Compliance Effects of the Robust New Technology?

Will New U.S. Privacy Regulations Be Too Expensive for Small Businesses?

Dish To Pay $280 Million in Penalties for TCPA Violations

Consumer Data Privacy: Why We Need A (Single) Federal Law

Mark Zuckerberg says he wants stricter European-style privacy laws — but some experts are questioning his motives

SECURITY CAMERAS

Aibo's dark side: Why Illinois bans Sony's robot dog

The state's Biometric Information Privacy Act prevents Sony from selling it there.

Utah is the first in the nation to have an electronic data privacy law

Most Companies Aren't Ready for California's Tough New Privacy Law

GDPR and CCPA: Strategic Imperatives for Marketing

Privacy becomes a selling point for tech, with Apple and Microsoft leading the way

A New Spin on Song-Beverly Act Litigation

Facebook, Google And Apple Seek Dismissal Of Lawsuit Over Location Tracking

California Attorney General wants to give consumers the right to sue if their privacy is breached

Pennsylvania Wiretapping Law

Supreme Court challenges $8.5M class-action privacy settlement against Google

Strict new Florida Biometric Information Privacy Act proposed in legislature

Why do 12 states still make it illegal to tape people without their knowledge?

New Jersey bill would broaden PII requiring breach notification

ERI's John Shegerian Calls Anthem's Record HIPAA Settlement a 'Warning for the Entire Healthcare Industry'

UCLA Health Settles $7.5M Lawsuit Over Data Breach

FEMA violated privacy law by releasing info of 2.3 million survivors of hurricanes, wildfire

Canadian sex toy maker accused of secretly collecting intimate data settles $5M lawsuit

Privacy class action landscape generally

- Abusive class actions and pre-suit demand letters.
- Who are the lawyers?
- Who are the plaintiffs and claimants?
- Judicial recognition of the landscape.
- Balance risk with business objectives.
- Key is to ensure awareness of new technology tools and programs being considered by the business.
- Black-and-white views unrealistic.

Privacy class action landscape generally

- Avoid being roadblock to the business.
- Educate internal stakeholders.
- Heightened awareness of practices in California, Illinois, New Jersey, Florida and Washington.
- Vendor management:
  - Size and financial health of vendors.
  - Indemnification provisions.
  - Insurance.
- Arbitration agreements/class waivers.
- Outside counsel perspective.

Common attributes of a privacy related class action

- Statute providing for significant damages with no cap.
- Plaintiffs' lawyers prefer no actual harm requirement (*e.g.*, TCPA, BIPA under *Rosenbach*; compare with TCCWNA, VPPA claims).
- Find the case then find the plaintiff.
- Always a story.
- Parroting language of the pertinent statute.
- Provocative general allegations.
- Leveraging discovery (fishing expedition).

Privacy class action landscape generally

- Stay calm
- Find the story
- Summary judgment to cut in front of class certification
- Know their playbook
- Inform the court as early as possible
- Become a “hard target”
- Go on offense
- Contain discovery
- Litigate to a larger audience of the plaintiffs’ class action bar
- Shut down as early as possible
- Depose the plaintiff
- Find leverage

TEXT MESSAGING/TCPA UPDATE

Jay Edelson Retweeted

Edelson PC @edelsonpc · Apr 15

@jayedelson: "this $925 million verdict is the largest standing verdict in a privacy case. It sends a powerful message to the defense bar that our firm and others are eager to try privacy cases and that juries are sympathetic."

Background

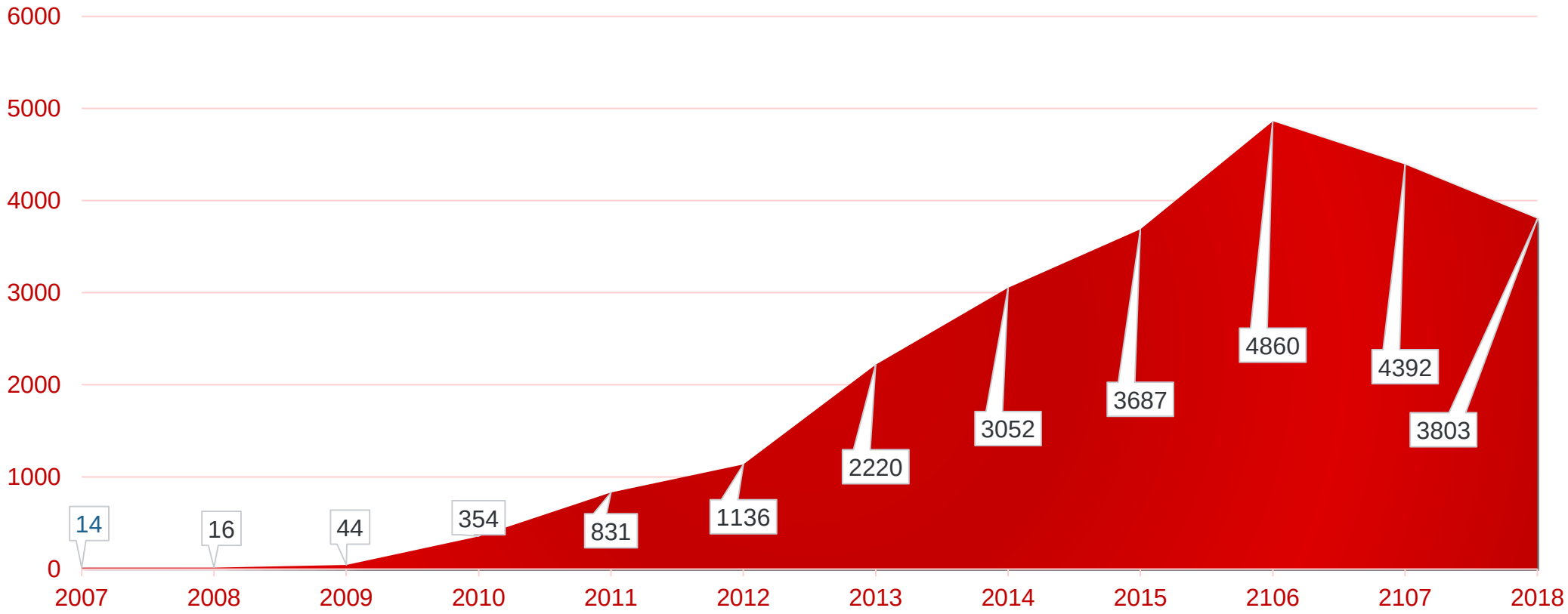
- Companies are increasingly using text messaging to convey helpful and desired communications to consumers.
- These types of text programs have been the source of litigation activity under the Telephone Consumer Protection Act, 47 U.S.C. § 227, *et seq.* (TCPA).

Statutory Damages

The TCPA provides for statutory damages of $500 to $1,500 per violation, which can be aggregated with no cap.

- The heightened damages of $1,500 per violation are awarded where a defendant's conduct is shown to have been "willful."
- To prove a willful violation, some courts have found that a plaintiff must establish that a defendant intended to text the plaintiff knowing that he or she did not consent to the text, while others have held that a plaintiff must show that a defendant placed a text with knowledge that it was violating the TCPA.

TCPA cases filed by year



Positive changes on the horizon

ACC Int'l v. FCC, 885 F.3d 687 (D.C. Cir. 2018)

On March 16, 2018, the D.C. Circuit issued its long-awaited decision in an appeal challenging the FCC's controversial July 2015 Declaratory Ruling, which significantly expanded liability under the TCPA.

The D.C. Circuit decision addresses:

- "Automatic Telephone Dialing Systems" (ATDS)
- Reassigned Numbers
- Revocation of Consent
- Health Care Communications

The Definition of an ATDS

TCPA

Equipment that "has the capacity" to:

- "[S]tore or produce telephone numbers to be called, using a random or sequential number generator."
- "[D]ial such numbers."

FCC

"[T]he capacity of an autodialer is not limited to its current configuration but also includes its potential functionalities."

The FCC's sole example of what would not constitute an ATDS: an old-fashioned rotary-dial phone.

The Definition of an ATDS

The D.C. Circuit squarely rejected the FCC's expansive reading and handed petitioners a complete victory on this issue, sending the FCC back to the drawing board.

The court found that:

- The FCC's reading "would appear to subject ordinary calls from any conventional smartphone to the Act's coverage an unreasonably expansive interpretation of the statute."
- "It cannot be the case that every uninvited communication from a smartphone infringes federal law and that nearly every American is a TCPA-violator-in-waiting, if not a violator-in-fact."
- It is "untenable" for the FCC to interpret the term "capacity" to include "potential functionalities" or "future possibility" and the FCC's ruling was unreasonable, arbitrary and capricious.
- There is, however, a circuit split in the courts [*e.g.*, Third and Ninth Circuits are diametrically opposed] and we await the FCC's imminent order interpreting the term per the D.C. Circuit's ruling.

Reassigned Numbers

Wireless numbers that, unbeknownst to the caller, have been reassigned from a consenting party to another, nonconsenting party.

Why does it matter?

Because a key defense to the TCPA is consent. Calls “made with the prior express consent of the called party” do not violate the TCPA.

Who is the “called party”?

The actual recipient of the call or the intended recipient of the call? The FCC interpreted “called party” narrowly by excluding the “intended recipient” from the definition.

The FCC also adopted a safe harbor –

A “one-call exemption” that shielded callers from TCPA liability for the first post-reassignment call. After that one call, the caller would be deemed to have “constructive knowledge” of the reassignment, regardless of whether that call actually informed the caller of the reassignment.

Reassigned Numbers

The D.C. Circuit

- Upheld the FCC's narrow interpretation of "called party."
- Set aside the FCC's "treatment of reassigned numbers as a whole" because the one-call safe harbor was "arbitrary and capricious."

Reassigned Numbers

Why business should remain optimistic:

- We expect the FCC will move with all deliberate speed to craft a workable rule that will withstand appellate scrutiny.

- The FCC considered – and granted – the request for a reassigned number database.
  - "Creating a comprehensive repository of information about reassigned wireless numbers."
  - A potential "safe harbor for callers that inadvertently reach reassigned numbers after consulting the most recently updated information."
  - The database is being developed but it will likely take some time to get it up and running.

Revocation of Consent

In its Declaratory Ruling, the FCC concluded that consumers may revoke consent at any time through any reasonable method that, based on “the totality of the facts and circumstances,” expresses “a desire not to receive further messages.”

Revocation of Consent

The D.C. Circuit upheld the FCC's ruling on revocation of consent, finding that:

- The Declaratory Ruling "absolves callers of any responsibility to adopt systems that would entail 'undue burdens' or would be 'overly burdensome to implement.'"
- Businesses would "have no need to train every retail employee on the finer points of revocation."
- Businesses should develop "clearly defined" and "easy-to-use" opt out or revocation methods, so that "any effort to sidestep the available methods in favor of idiosyncratic or imaginative revocation requests might well be seen as unreasonable."

Revocation of Consent

"Nothing in the Commission's order . . . should be understood to speak to parties' ability to agree upon revocation procedures."

- The D.C. Circuit did not disturb the Second Circuit's ruling in *Reyes v. Lincoln Auto. Fin; Servs*., 861 F.3d 51 (2d Cir. 2017), which held that a consumer cannot unilaterally revoke his or her consent when that consent is given as bargained-for consideration in a bilateral contract.

- Courts in other circuits may begin following suit. See *Bartori v. Credit One Financial*, No. 16-12652, 2018 WL 2012876 (N.D. Ohio Apr. 30. 2018) (granting summary judgment because plaintiff's efforts to unilaterally revoke consent were improper in light of the valid cardholder agreement between the parties).

Takeaways and risk mitigation strategies

While the recent regulatory rulings make it virtually impossible to ensure perfect compliance with the TCPA, there are steps that every business should consider to substantially mitigate risk.

- Ensuring that all texting activities are run through in-house legal pre-launch.
- Obtaining proper consent.
- Maintaining records of proper consent.
- Implementing a double opt-in process as endorsed by the FCC.
- Maintaining active vendor management.
- Scrubbing for reassigned numbers.
- Honoring revocation requests.
- Monitoring the national Do-Not-Call Registry and maintaining an internal do-not-call list.
- Conducting regular TCPA compliance audits of internal operations and vendors.

BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

Overview

No universal definition of biometric data, but generally refers to unique and immutable information that can be used to identify a particular person.

Referred to in state laws as “biometric identifiers,” which generally include fingerprints, voiceprints, eye and/or face scans.

Broader definitions include “biometric information,” which can mean any information derived from a biometric identifier that can likewise identify a particular person.

Present uses across industries:

- Employee monitoring
- Employee tracking
- Identification confirmation
- Frictionless transactions on mobile app
- Gaming and AR
- Payment verifications
- Security measures
- Physical & digital access/restrictions
- Customer experience
- Wearable tech
- Wellness programs
- Health assessments.

Lack of one comprehensive federal biometrics law

- Patchwork of federal laws that apply in particular circumstances (*e.g.*, HIPAA and GINA).
- Note Section 5 of the FTC Act and FTC Report titled, “Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies.”
- Proposed legislation is in committee: Senate Bill 2728, proposal for a Social Media Privacy Protection and Consumer Rights Act of 2018.
- Other federal agencies may seek to regulate biometric data for security and privacy purposes.
- In the absence of a comprehensive federal law, companies have to adjust to a growing number of state laws and court decisions (Ill., Wash., Texas).
  - Regulate the collection, storage, use and disclosure of biometric data; contain consent provisions and provide for enforcement through private right of action (Ill.) or state AGs (Texas and Wash.).
  - Proposals and amendments have percolated in Ark., Del., N.Y., N.J., Ill..

Illinois Biometric Information Privacy Act (BIPA)

- Passed in 2008 by the Illinois General Assembly in response to Pay By Touch bankruptcy.
- Increase in class action activity under BIPA over the last couple of years, led by Jay Edelson of Edelson PC.
- Minefield of litigation risk for companies that use facial recognition, fingerprinting and/or iris or retina scanning technology, and do not fall into one of the excluded categories under the statute.

The BIPA – defining biometric data

The BIPA applies to any "private entity" that possess "biometric identifiers" and/or "biometric information."

The BIPA defines "biometric identifiers" to include "a retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry."

The BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify an individual."

Photos expressly excluded – but…

The BIPA – exclusion for certain health care data

"Biometric Identifiers" under BIPA do not include:

- Donated organs, tissues or parts as defined in the Illinois Anatomical Gift Act, or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants.
- Information captured from a patient in a health care setting or information collected, used or stored for health care treatment, payment or operations under HIPAA.
- Biological materials regulated under the Genetic Information Privacy Act.
- An X-ray, roentgen process, computed tomography, MRI, PET scan, mammography or other image or film of the human anatomy used to diagnose, prognose or treat an illness or other medical condition or to further validate scientific testing or screening.

The BIPA – requirements and restrictions

- Disclose in writing to an individual what biometric identifiers or information are being collected, why they are being collected and the length of time they will be collected or stored.
- Obtain written consent from an individual before collecting his or her biometric identifiers or information.
- Provide a publicly available written retention policy regarding the permanent destruction of biometric identifiers and information with specific requirements.
- Refrain from selling biometric identifiers or information.
- Destroy biometric identifiers and information within three years of an individual's last interaction with the entity, or as soon as the purpose for the collection of that person's biometric data is satisfied, whichever is earlier.
- Refrain from disclosing biometric identifiers or information, except in limited circumstances.
- Protect biometric identifiers and information in a reasonable manner that is at least as protective as the manner in which the entity protects other confidential and sensitive information.

The BIPA – early class actions & familiar players

- Comparison with TCPA and similar statutes that led to litigation explosion.
- Early BIPA class actions were filed, in large part, against social media and technology companies challenging the allegedly noncompliant use of facial recognition technology.

The BIPA – *Rosenbach v. Six Flags*

ISSUE

What does it mean to be an “aggrieved” person entitled to seek liquidated damages and injunctive relief under the BIPA?

HOLDING

On January 25, 2019, the Illinois Supreme Court ruled that a plaintiff does not need to allege an “actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an aggrieved person” entitled to seek injunctive relief and liquidated damages of up to $5,000 per alleged violation of the BIPA.

The BIPA – *Rosenbach v. Six Flags*

HOLDING

- In the court's view of statutory construction, the word "aggrieved" means suffering an infringement of a legal right without more.
- The court also stated that a violation of the BIPA's requirements, in and of itself, is an "injury" that is "real and significant" because, "when a private entity fails to adhere to the statutory procedures …, 'the right of the individual to maintain his or her biometric privacy vanishes into thin air.'"
- Finally, the court stated that the "preventative and deterrent" purposes of the BIPA would not be served if plaintiffs had to suffer "some compensable injury" beyond a statutory violation before "they may seek recourse."

Consequences of *Rosenbach*

- Conflicts with prior judicial interpretations of what it means to be "aggrieved" by an alleged statutory violation.
- Takes a much broader view of statutory standing than would be permitted under the U.S. Supreme Court's approach to jurisprudential, Article III injury-in-fact requirements.
- Creates the potential for potentially annihilating and disproportionate liability in the absence of any resulting harm.
- Will likely perpetuate the refiling in Illinois state court of BIPA cases dismissed in federal court on Article III grounds.
- Has resulted in a significant increase in putative BIPA class actions in Illinois state court.

Takeaways and Risk Mitigation Strategies

- Threshold issue – arbitration in employment and consumer contexts.
- Publicly available, written retention schedule.
- Privacy assessment or audit in privileged manner.
- Process for informing consumers and employees about collection, storage and use of biometric data and obtaining requisite consent.
- Awareness of the issues generally; educate internal clients.
- Ensure data is adequately protected.
- Develop, implement and maintain written policies and train employees.
- Refrain from selling or profiting from biometric data.

Takeaways and risk mitigation strategies

- Diligence with vendors and vendor contracting; related insurance and indemnification.
- Document written consent.
- Ensure privacy policies = practices.
- Save biometric data only for as long as it is needed.
- Collect what you need – Is there a way to achieve the same goals through less sensitive data? Is there a viable, cost-effective way to exclude Illinois from biometric programs for the time being?
- Address biometric data in written incident response plans for data breaches.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Overview

In June 2018, Governor Brown signed the CCPA into law. It is slated to become effective in January 2020.

In its current form, the CCPA creates a private right of action for California residents if their unencrypted or unredacted personal information is compromised because of a business's failure to implement reasonable security measures.

- A plaintiff may seek his/her actual damages or statutory damages between $100 and $750 per consumer per incident, with no cap on aggregation.

The CCPA empowers the Attorney General to pursue cases against businesses for penalties of up to $7,500 per violation for intentional violations of the statute.

Overview

In general, the CCPA grants California residents the right to:

- Know what personal information is being collected about them.
- Know whether their personal information is sold or otherwise disclosed and to whom.
- Say no to the sale of their personal information.
- Access their personal information and request deletion under certain circumstances.
- Receive equal service and price, even if they exercise their rights under the statute.

Whose personal information is covered?

- The CCPA protects the personal information of consumers.
- For purposes of the CCPA, a “consumer” means any natural person who is a resident of California as defined in tax provisions.
- That includes:
  - Every individual in California who is not there for a temporary or transitory purpose.
  - Every individual who is domiciled in California, but is outside of California for a temporary or transitory purpose.

What personal information is covered?

- The CCPA takes a broad view of personal information.
- Includes any information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked with a particular consumer or household, directly or indirectly.
- Includes information such as name, postal address, social security number, education information, consumer preferences, biometric data, etc.
- Definition is subject to expansion under Attorney General's regulations.

Exclusions:

- publicly available information;
- de-identified information; and
- aggregate consumer information.

What businesses/ entities are regulated?

The CCPA governs businesses (for-profit entities) that:

1. Collect consumers' personal information, or on whose behalf such information is collected, and that determine the purposes and means of processing that information.

2. Meet one of three criteria:

   (a) have annual gross revenue above $25 million

   (b) alone or in combination annually buy, receive for commercial purposes, sell, etc. the personal information of 50,000 or more consumers, households or devices

   (c) derive 50 percent or more of their annual revenue from selling consumers' personal information. Entities that either control or are controlled by such businesses are also covered by the Act.

The CCPA also restricts businesses in sharing personal information with service providers.

What information must be provided to consumers upon request?

- The categories and specific pieces of personal information the business has collected about that consumer.
- The categories of sources for which the personal information is collected.
- The business purpose for which the personal information is collected.
- The categories of third parties with whom the business shares the consumer's personal information.
- The categories of personal information that the business sold or disclosed about the consumer for a business purpose.

Subject to potential extensions, businesses have 45 days to respond to such a request and the response must cover the prior 12-month period.

The right to delete information

Consumers have the right to request that a business and its service providers delete their personal information. Unclear how information is to be deleted and how such deletion would be tested/verified.

Several potentially broad exceptions

- To complete the transaction or service for which the information was collected.
- To detect security incidents, protect against malicious, deceptive/fraudulent or illegal activity, or prosecute those responsible for that activity.
- To fix or identify errors.
- To exercise free speech.
- To engage in certain types of research if the consumer has provided informed consent.
- To comply with certain sections of the California Electronic Communications Privacy Act.
- To enable solely internal uses that are reasonably aligned with the consumer's expectations.
- To comply with legal obligations.
- To use internally in a lawful manner consistent with the context in which the information was provided.

The right to opt out

Consumers have the right to opt out of the sale of their personal information to third parties.

- Opt-outs cannot be solicited for reauthorization for 12 months after opting out.
- Businesses must provide a “Do Not Sell My Personal Information” link on their website homepage to enable consumers to opt out.
- Consumers must be able to opt out without having to create an account with the business.
- Minors or their guardians have opt in rights.
- Open questions remain regarding sales to advertisers where access to information about specific individuals is sold without providing specific information from those individuals.

Recent Activity

- The Attorney General's Office (AGO) has until July 1, 2020, to adopt CCPA-related regulations. Enforcement of those regulations has been postponed to the earlier of six months from the date the AGO adopts its regulations or July 1, 2020.
- Proposed amendments suggest removing the various prerequisites for a consumer filing a private right of action, including providing the AGO with notice.
- "Protected health information" as defined under HIPAA that is collected by a HIPAA-covered entity or business associate is exempted. HIPAA-covered entities are exempted to the extent that they maintain patient information in the same manner as medical information or protected health information in accordance with CMIA and HIPAA, as applicable.
  - Questions remain as to whether a business offering a mobile health app that collects information directly from individuals may take advantage of these exemptions.
- A bill (AB 981) is pending that would exempt insurance companies and banks from compliance with the CCPA.
- As of April 18, 2019, there are 16 proposed amendments to the CCPA pending in the legislature.

Takeaways and risk mitigation strategies

- Determine if you collect, maintain or hold California residents' personal information or if an entity you control or that controls you does so.
- Consider establishing a specific role for addressing and following requirements regarding personal information.
- Create a data map that identifies who collects/uses/shares personal information, for what purpose and where and how that data is stored/accessed.
- Incorporate a recognized security framework to ensure the business is employing reasonable security measures.
- Encrypt or redact consumers' personal information when collected, stored or transmitted.
- Draft strong contracts with service providers to mitigate CCPA exposure.

A reminder about the benefits of ACC membership . . .

- Free CLE, like the one you're attending right now
- Roundtables
- Networking meetings
- Special events
  - Spring Fling, Fall Gala, Diversity Summer Program, Golf Outing, Pro Bono clinics, Charity Softball Game & Family Fun Day, and more!

- Access to ACC resources, including:
  - ACC Newsstand (customizable updates on more than 40 practice area)
  - ACC Docket Magazine
  - InfoPAKs
  - QuickCounsel Guides

For more information or to refer a new member, see your hosts today or contact Chapter Administrator, Chris Stewart, at ChrisStewart@ACCglobal.com.

ACC Association of Corporate Counsel
GREATER PHILADELPHIA