WINSTON & STRAWN LLP

REGULATED PERSONAL INFORMATION

A New Privacy Paradigm: Risks, Trends, and Best Practices in the Shifting Landscape of U.S. Privacy Laws

February 16, 2023

SPEAKERS

ALESSANDRA SWANSON
Partner and Co-Chair,
Global Privacy & Data Security Practice
Chicago

SEAN WIEBER
Partner and Co-Chair,
Global Privacy & Data Security Practice
Chicago

MODERATOR

DANIELLE WILLIAMS
Managing Partner, Charlotte
Intellectual Property Partner
Charlotte

WINSTON & STRAWN LLP

Overview

Agenda

- The Privacy Awakening: The Regulatory Landscape and How We Arrived Here
- The Driving Forces For What Comes Next
- How to Think About Managing Privacy-Related Risks
- Questions

Our Goal For Today's Presentation

- As privacy is a rapidly evolving field, there will rarely be clear-cut answers to the complicated legal questions your organization will face.
- Therefore, our goal today is to provide you with meaningful context about the current state of privacy and a primer on how to navigate associated risks.

WINSTON & STRAWN LLP

THE PRIVACY AWAKENING

The Regulatory Landscape and How We Arrived Here

Current State of U.S. Privacy Law

- Prior to 2018, outside regulated industries like health care and financial services, there were no comprehensive privacy laws regulating personal information in the United States.
- Today, with California leading the way, there are five states with complicated and sometimes conflicting regimes that have radically shifted how businesses must manage their consumer, employee, and customer personal information.

Current State of U.S. Privacy Law

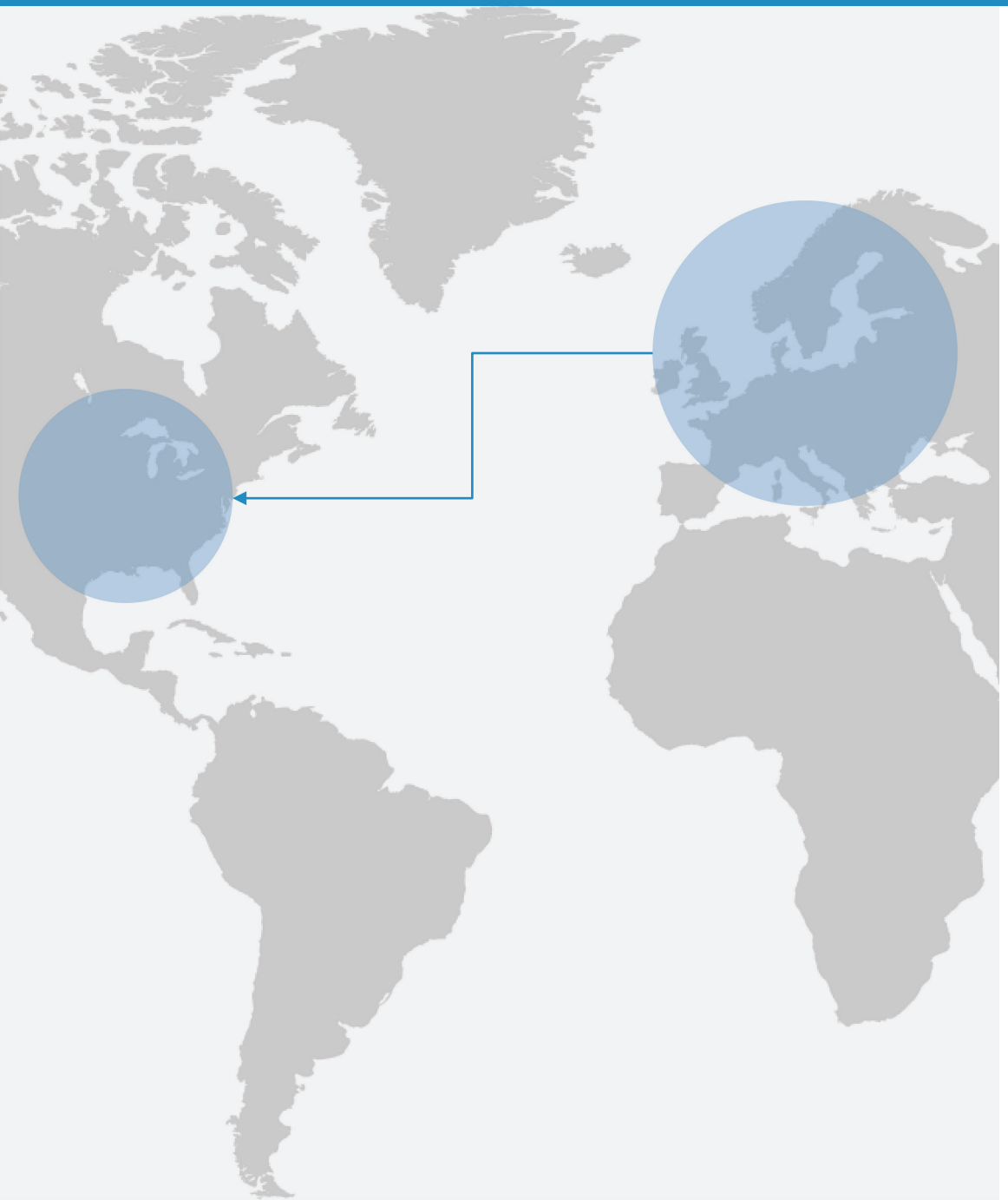
- Regulators have responded to increasing consumer concern related to the use and disclosure of personal information by introducing and passing significant legislation, such as CCPA, VCDPA, etc.
- Plaintiffs' attorneys have seized upon this focus on privacy by pursuing claims under laws that received almost no interest prior to 2015, including BIPA and CIPA.

This Has Led to the Morass of Acronyms and Buzzwords…

Right to be "Forgotten" TCPA DNC Lists CCPA CIPA Prior Express Consent Written Release Robocalls BIPA Biometric Identifiers FSCA Autodialers Aggrieved Person Standard of Care Processing Data WESCA Personal Data VPPA Invasion of Privacy Aggregation and Anonymization

… And Now We Have the Perfect Storm.

- Aggressive Plaintiffs' Bar
- Uncapped Statutory Damages
- Strict Liability and Tough to Dismiss at Pleading Stage
- Bet-the-Business Class Action Damages Calculations
- Vague and Ambiguous Statutes
- Rapidly Developing Case Law
- Ever-Changing Regulatory Landscape



How Did We Get Here?

- Europe led the way with the General Data Protection Regulation ("GDPR"), which went into effect in 2018 and codified long-standing European privacy principles.
- In the EU, privacy is considered a "universal human right."
- Since 2018, regulatory fines under the GDPR have grown exponentially – including a 168% surge in of fines in 2022, equating to over $3.1 billion in fines.

"Americanization" of EU Privacy Regulation

- The US lacks a federal generally applicable privacy regulation akin to the GDPR
  - The processing of personal information is governed by a patchwork of state and federal laws
  - Up until the CCPA, these laws were industry- or use case-specific
- In the last decade, US legislatures have married EU privacy principles with a private right of action and statutory damages
  - Thus, in many cases, consumers are able to enforce US privacy laws alongside regulators

The Driving Forces For What Comes Next

Trends That are Driving Change Now

Consumers want CONTROL over how their personal information is processed, and this has spurred regulators into action. In particular, consumers want to assert some authority over:

PROCESSING

- How their personal information is collected, used, and disclosed.

CONTACT

- Who can contact them and by what means.

BIOMETRICS

- When and how biometric information can be collected and used.

MONITORING

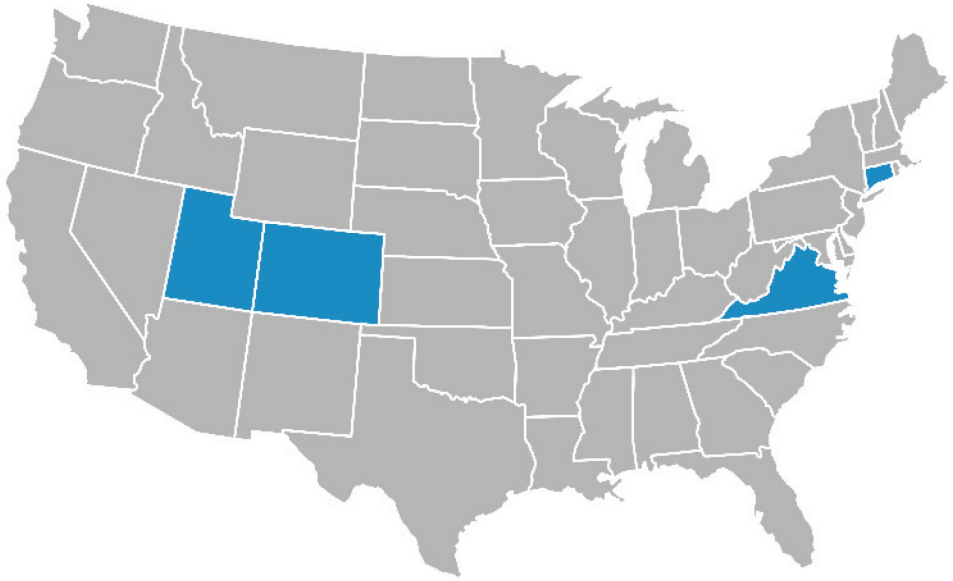
- What means are used to monitor their communications.

Processing

Increased Oversight of Processing Activities

- California, Virginia, Colorado, Connecticut, and Utah all have comprehensive privacy laws that go into effect in 2023
- The most significant of these, CPRA, went into effect 1/1/2023, but will not be enforced until 7/1/2023
- Regulations were “finalized” 2/3/2023 (with more regulations incoming)
- CPRA builds on the CCPA, including creating new and expanded rights for consumers
- Creates the concept of “sensitive” personal information
  - SSN, government ID, geolocation, demographic information, genetic data, etc.

Virginia, Colorado, Connecticut, Utah



- These laws share a similar mold and are largely CPRA "light"
  - Generally, these laws apply only to consumers and contain CPRA-type rights
  - Do not contain a private right of action, even for data breaches
- Virginia Consumer Data Protection Act (effective 1/1/2023)
- Colorado Privacy Act (effective 7/1/2023)
  - Rulemaking on regulations still in process
- Connecticut Data Privacy Act (effective 7/1/2023)
- Utah Consumer Privacy Act (effective 12/31/2023

Consumer Rights Over Processing Activities

- Right to Know
- Right to Access
- Right to Deletion
- Right to Correction
- Right to Opt Out of the Sale or Sharing of Personal Information
- Right to Limit Use or Disclosure of Sensitive Personal Information
- Right to Equal Services and Prices

WINSTON & STRAWN LLP

Contact

TCPA Compliance

- Complicated rules + always-evolving legal landscape + astronomical damages = **significant risk**
- With a private right of action and statutory damages of between $500 and $1,500 per violation (in addition to attorneys' fees), TCPA litigation has historically resulted in massive class action settlements
- Prior express **written** consent (PEWC)
  - The "gold standard" for consent–but PEWC requires very specific language
  - Required for "advertising" or "telemarketing" calls or texts sent via ATDS
  - Be wary of click-wrap agreements–consent language must be prominent
- Prior express consent (PEC)
  - PEC can be obtained in a variety of ways: in person, in writing, over the phone
  - PEC required for "transactional" or "informational" calls and texts
    - Caution! Dual-purpose texts are a trap for the unwary

Facebook v. Duguid

- In April 2021, SCOTUS significantly narrowed the types of dialing equipment considered "automated telephone dialing systems." (ATDS)
  - Per SCOTUS, the device must have the "capacity to use a random or sequential number generator to either store or produce phone numbers to be called."
  - Mere capacity to store and dial numbers is insufficient to qualify as an ATDS.
- This decision significantly limited the instances in which PEWC is required.

Plaintiffs' Bar's Response

- After an initial decrease in TCPA litigation following *Facebook*, the plaintiffs' bar has shifted its focus.
- Claims are now focusing on violations of the TCPA's do-not-call-list provisions and the use of prerecorded calls (which do not require use of an ATDS).
- In addition, plaintiffs are using "mini-TCPA" laws at the state level.
  - These laws contain similar requirements to the TCPA but were unaffected by the *Facebook* decision.

Biometrics

Biometric Information Privacy Act (BIPA)

- Passed by the Illinois General Assembly in 2008
- Restricts how private entities collect, retain, disclose, and destroy biometric identifiers and biometric information

- **A unique private right of action**

The Stakes Are High

- **Statutory Damages**
  - $1,000 for each “negligent violation”
  - $5,000 for each “intentional” or “reckless” violation
  - **Accrual:** Illinois Supreme Court has agreed to hear a case in 2022 about the accrual of BIPA violations
- **Class Size**
  - Based on the most recent case law in Illinois, the statute of limitations is **five years**
- **Large Settlements**
  - Many cases have been settling for over **$1,000 per class member**
  - **Facebook case:** Settled for $650 million
  - **BNSF:** First major case brought to trial, resulting in a $248 million award for “technical” violations of the law

"Strict Liability"

- No case law on what makes a violation negligent or reckless/intentional sufficient to trigger statutory damages of $1,000 or $5,000, respectively
  - May change in 2023 with *White Castle*
- Difficult argument for defendants who violated the statute to say they were not at least negligent in doing so:
  - "BIPA was enacted in 2008 and numerous articles and court filings about the Act's requirements were published before Defendant employed [Plaintiffs]. And Defendant apparently became aware of BIPA at some point prior to Plaintiffs filing this lawsuit, as it attempted to obtain retroactive consent from Lenoir for the collection of her fingerprint data. These facts plausibly suggest that, at a minimum, Defendant was negligent for its earlier failures to comply with BIPA."
    Lenoir v. Little Caesar Enterprises, 2020 WL 4569695 (N.D. Ill. Aug. 7, 2020)

Other States and Municipalities

- Texas Facebook suit
- Other states continue to propose new biometric legislation
- New York City Mini BIPA
  - Private right of action for use of FRT in commercial establishments
- New York ban on “mandatory” biometric collection from employees
- Other cities have banned or limited use of FRT:
  - Portland, Oregon
    - First litigation brought under this regulation in 2023
  - Oakland, California
  - Berkeley, California
  - Cambridge, Massachusetts

Monitoring

CIPA, WESCA, VPPA, and Similar Laws

- Plaintiffs have had recent success applying eavesdropping and wiretapping laws against websites using "session replay" software or chatbots
- The California Invasion of Privacy Act prohibits intentional wiretapping, or willfully learning the content of communications in transit, or attempting to use or communicate information obtained by either of those means
  - In *Javier v. Assurance IQ, LLC*, the 9th Circuit reversed dismissal of a claim that using a tracking tool to create a video recording of a website visitor filling out an onboarding form violated CIPA
  - The court found that, under CIPA's two-party consent requirements, CIPA requires prior express consent of all parties before information is collected
  - CIPA provides a private right of action and statutory damages up to $5,000 per violation

CIPA, WESCA, VPPA, and Similar Laws

- Similar claims have been brought under Pennsylvania's Wiretapping and Electronic Surveillance Act and Massachusetts's Invasion of Privacy Act
- Plaintiffs have sued website operators under the Federal Video Privacy Protection Act for use of third-party tracking tools (e.g., Meta Pixel)
  - VPPA was originally intended to prevent the disclosure of personal information that identifies an individual as having requested or obtained specific video material
  - These claims have implicated HIPAA as well, given the trackers' collection of information on websites/apps maintained by HIPAA-covered entities.
  - VPPA provides up to $2,500 per violation

WINSTON & STRAWN LLP

How to Think About Managing Privacy-Related Risks

Privacy Risk is Interrelated Across The Spectrum

Understand Where Risk Exists

- Conduct a diligence exercise to understand where your sensitive data "lives"
- Conduct a data-mapping exercise to track how this information flows into, through, and out of your organization
- Dispose of unnecessary data – and make sure your vendors do too
- Talk to your business teams to assess what they are doing with personal information today, tomorrow, and two years from now

Address Potential Sources of Risk

- Commercial contract terms
- Oversight of vendors
- Internal understanding of privacy requirements
- Data security infrastructure
- Insurance

Be Prepared to Act

- View data-use scenarios through the eyes of a regulator, consumer, or plaintiff's attorney
- Undergo data security risk exercises
- Establish processes to address privacy complaints
- Create and execute upon remediation plans

Questions?

WINSTON & STRAWN LLP

Presenter Bios

Services
Government Program Fraud, FCA, and Qui Tam Litigation
Health & Welfare Benefits
IP/IT Transactions & Licensing
Intellectual Property
Privacy & Data Security
Regulated Personal Information

Sectors
Consumer Products
Financial Services & Banking
HIPAA and HITECH
Health Care & Life Sciences
Health Care Litigation & Investigations
Health Care Privacy & Data Security
TNT

Bar Admissions
Illinois

Education
DePaul University, JD, 2009
Northwestern University, BA, 2005

ALESSANDRA SWANSON

Co-Chair, Global Privacy & Data Security and Regulated Personal Information Practices
Chicago
+1 (312) 558-7435
Aswanson@winston.com

Alessandra is a co-chair of Winston's Global Privacy & Data Security and Regulated Personal Information practices and counsels clients on significant matters related to the collection, processing, and protection of personal information.

Alessandra is a former federal privacy regulator and primarily focuses her practice in the areas of regulated personal information, privacy and data security counseling, security breach response and regulatory defense, corporate advisory services and outsourcing, and large-scale commercial contracting. Prior to joining Winston, Alessandra spent five years with the U.S. Department of Health and Human Services – Office for Civil Rights, where she was involved in a number of high-profile privacy investigations and settlements.

Alessandra has counseled some of the country's most well-known health care companies, brands, retailers, media companies, and e-commerce platforms regarding their compliance with privacy and data security laws. She has helped clients develop privacy compliance programs, employee training, and security incident response plans; undertake information security assessments; implement privacy-by-design processes; create internal and consumer-facing privacy disclosures; assess software platforms and new technologies for privacy and security issues; and leverage new technologies to reach consumers.

Services
Advertising & Consumer Protection
Class Actions
CCL
Government Investigations
Litigation
Privacy & Data Security
Regulated Personal Information
White Collar, Regulatory Defense & Investigations

Bar Admissions
Illinois

Court Admissions
Central District of Illinois
Northern District of Florida
Northern District of Illinois
U.S. Supreme Court
USCA – 7th Circuit
USCA – 9th Circuit

Education
Chicago-Kent College of Law, JD, 2007
Northwestern University, BA, 2002

SEAN WIEBER

Co-Chair, Global Privacy & Data Security and Regulated Personal Information Practices
Chicago
+1 (312) 558-5769
Swieber@winston.com

Sean focuses his practice on a variety of complex commercial and class action litigation matters. As Co-Chair of Winston's Global Privacy & Data Security and Regulated Personal Information (RPI) practices, Sean has vast experience advising clients on privacy, data breach, and consumer matters (brought as class actions or as individuals) under various federal and state laws that are primarily enforced through private right of action, such as the Telephone Consumer Protection Act (TCPA), the Illinois Biometric Information Privacy Act (BIPA), the California Consumer Privacy Act (CCPA), the California Invasion of Privacy Act (CIPA), the Florida Telephone Solicitation Act (FTSA), the Florida Security of Communications Act (FSCA), and the Video Privacy Protection Act (VPPA).

Sean also regularly conducts highly sensitive internal investigations for publicly traded and privately held companies, municipalities, and volunteer and nonprofit organizations into issues involving employee misconduct, accounting irregularities, whistleblower complaints, the Computer Fraud and Abuse Act, and potential violations of the Foreign Corrupt Practices Act (FCPA) and other anti-bribery laws.

Sean has been recognized as a legal "trailblazer"—in that after observing the ever-increasing onslaught of class actions initiated under privacy and consumer protection laws, he knew there had to be a better way of separating the "wheat from the chaff"—that is, assessing very early in a case's life cycle which matters were truly "bet-the-company" and should be litigated as such, versus those that were ripe for dismissal almost immediately, or, alternatively, were better suited for a negotiated resolution. As such, Sean has developed a methodical and tenacious approach when assessing his clients' matters—operating collaboratively and with transparency with stakeholders on both sides of the "v"—ultimately fostering the proper disposition of disputed issues in an efficient and effective manner.

WINSTON
&STRAWN
LLP