March 25, 2022

Priority Areas for Privacy Practitioners

Arianna Evers
Special Counsel, WilmerHale

Ali Jessani
Senior Associate, WilmerHale

Alex Altman,
Senior Associate, Arnold & Porter

Privacy+ Security Forum

Overview

Setting the Scene

Privacy+ Security Forum

- Enormous range of developments in the privacy universe, at the state, federal, and international levels
- Different jurisdictions having overlapping, inconsistent requirements is creating unique challenges
- Creating increased complexity for companies and other entities operating across industry and country lines
- Real pressures for broader state laws (and, perhaps, a national law)
- Increasing focus on certain activities, with open questions as to how these activities are defined and regulated, as well as how the underlying concerns will be addressed
- Increased attention from wide range of regulators, looking to police existing law and make new laws/obligations

Agenda

1. State privacy laws: update and trends
2. State privacy laws: compliance checklist
3. Federal law developments
4. U.S. enforcement trends
5. Key international developments

State Privacy Laws: Updates and Trends

Privacy+ Security Forum

Updates and Trends

- California Consumer Privacy Act went into effect in January 2020
  - First comprehensive privacy law passed in the US
- Enforcement has been ongoing since July 2020
- Multiple states have proposed comprehensive privacy laws since the CCPA passed in 2018

Updates and Trends

- California voters passed California Privacy Rights Act in November of 2020; will amend the CCPA in January of 2023
- Virginia and Colorado passed their own comprehensive privacy laws last year
- Both will go into effect in 2023 (Virginia in January; Colorado in July)
- Some similarities to CCPA but also notable differences

Updates and Trends

- At least 15 states proposed comprehensive privacy legislation in 2022
- Utah (thus far) is the only state to have passed such a law
  - Will go into effect on December 31, 2023
- Some states passed a law in a single chamber (e.g., Florida, Iowa, Wisconsin) but those bills did not gain full support
- Sticking points seem to be enforcement provisions, penalties, private right of action

Updates and Trends

- California passed Genetic Information Privacy Act last year; went into effect in January
- Other proposals at the state level have aimed to regulate specific types of businesses or data:
  - Data broker bills similar to VT and CA
  - Biometric bills similar to BIPA in Illinois

State Privacy Laws: Compliance Checklist

Privacy+ Security Forum

State Law Compliance Checklist

- Many similarities in four state laws:
  - Broad definition of personal information or personal data
  - Individual data subject rights (e.g., access, deletion, correction)
  - Notice obligations (e.g., privacy policy disclosures)
  - Downstream contractual obligations (i.e., data processing agreements)

State Law Compliance Checklist

- Opt-in/opt-out for certain processing activities (e.g., “Do Not Sell” link)
- Privacy by design provisions (e.g., data minimization, purpose limitation)
- Reasonable security requirement

State Law Compliance Checklist

- Questions to ask:
  - What categories of information are being processed?
  - Who is the information being shared with and for what purposes?
  - What are my notice obligations in relation to this processing?
  - What are my contractual obligations for this information?
  - What safeguards am I implementing to protect this information?

Federal Law Developments

Privacy+ Security Forum

Overview of Federal Trends

- Congress continues to entertain numerous federal privacy proposals
- Some are comprehensive privacy proposals; others are more specific
  - E.g., non-HIPAA health data, children's data

U.S. Enforcement Trends

Privacy+ Security Forum

General Trends

- Federal Trade Commission (FTC) continues to provide visible and meaningful privacy and data security enforcement
- Tools are somewhat limited
  - FTC Section 5 authority
  - Specific consumer protection statutes and implementing rules
  - *AMG Capital Management*
- Democratic commissioners are looking for creative and aggressive ways to use the tools they have
- Technology is a priority, and there is an increasing linkage between privacy, big data, and broader consumer protection issues
- Disagreements between democratic and republican commissioners is playing out publicly in real-time, and will influence federal legislative debate

General Trends

Privacy + Security Forum

- FTC is engaging its full portfolio of tools and is thinking creatively about remedies
  - Notice to affected parties
  - Release from contractual arrangements
  - Data and algorithm deletion
  - Broad interpretations of existing rules
  - Extension of UDAP authority to state law violations
  - Penalty offense authority
  - Section 6(b) studies
- Shift away from notice and consent framework; focus on data minimization
- Focus on "data abuses"—harms to civil rights and equal opportunity, proliferation of misinformation, harms to competition, increasing labor exploitation

General Trends

- State Attorneys General ("AGs") continue to focus on privacy and data security in the absence of federal legislation, and are increasingly active in this space
- Many have dedicated teams for privacy and data security
- Certain AGs continue to be more actively players, either taking a leadership role in multistate investigations or "going it alone"
- Increased willingness to stretch general consumer protection authority to test out novel legal theories in the privacy and broader consumer protection space, even where there is no clear "win"

CafePress

- FTC settlement with CafePress
  - Security incidents affecting website www.cafepress.com
  - Specific representations about how information will be used will trump general privacy policy language
    - Pay attention to consent language and lesser seen representations
    - Test opt-outs or opt-ins to ensure functionality
  - Storage of information indefinitely without a business need
  - Deactivation of user accounts, but no data deletion
  - Consent order requires consumer redress

Children and Teen Privacy

- Children's Online Privacy Protection Act ("COPPA") and FTC COPPA Rule compliance continues to be a regulatory focus
  - Applies to online services (1) directed to children, or (2) with actual knowledge
- FTC settlement with Kurbo / WW International
  - Weight management service designed for children 8+, teens, and their families
  - Allegations (1) no neutral age gate, (2) failed to provide parental notice and obtain consent, and (3) kept children's PI indefinitely
  - Settlement required payment of $1.5M, the destruction of PI from accounts where parental notice/consent not obtained, and the destruction of "affected work product"

Children and Teen Privacy

- BBB Children's Advertising Revue Unit (CARU)
  - Self-regulatory body that monitors child-directed media to ensure compliance with CARU guidelines and COPPA
  - Change through voluntary compliance; where necessary, will refer cases to the FTC
  - Recent high-profile FTC hire and two new senior attorneys
  - Settlement with TickTalk
- Increased attention to teen privacy
  - Biden State of the Union
  - Federal legislative proposals
  - UK Age Appropriate Design Code; similar California proposal
  - TikTok and other state AG investigations

Dark Patterns

- Deceptive and manipulative user interfaces intended to influence users' online decisions
- CPRA and Colorado Privacy Act address dark patterns
- FTC enforcement policy statement
- State AG suit against Google over alleged dark patterns linked to location data practices
- FTC investigation into Amazon Prime

California

- CA AG has been actively investigating companies for CCPA violations – with enforcement just beginning
- Focus on technology companies and those in the advertising/marketing space
- Inquiries may seem more like fact-finding and learning about the industry
- Also using alleged CCPA violations as a hook to investigate conduct more broadly under the Unfair Competition law
- Public examples focused on low hanging fruit—deficient privacy policy, do not sell button, individual rights

Key International Developments

Privacy+ Security Forum

International Trends

- EU - GDPR – Cross-border Transfers vis-à-vis Google Analytics
- China – Impact of PIPL
- Japan – Amended APPI to Go Into Effect

<u>Common Thread</u>

Cross-border transfers and transfer impact assessments

GDPR – Cross-Border Basics

- Cross-border transfers may be made only to an "adequate jurisdiction" or under limited transfer mechanisms.
- "EU-US Privacy Shield" was one transfer mechanism until invalidated under CJEU's *Schrems II* decision in July 2020.
- Schrems II called into doubt viability of another mechanism: Standard Contractual Clauses (SCCs).
- European Commission adopted new SCCs in June 2021 in response to *Schrems II*.
- *Schrems II* also calls for "transfer impact assessments" and supplementary measures.

GDPR - Google Analytics

- Austrian DPA - December 22, 2021
  - Netdokter.at used Google Analytics (GA) and Standard Contractual Clauses (SCCs); cookie data sent in clear text.
  - Google qualifies as an “electronic communications service provider” subject to FISA Section 702
  - Per *Schrems II*, adequate protection of personal data cannot be ensured.
  - Decision was followed by a communication of the Dutch and Danish DPA: intended harmonized approach throughout the EU.

Google Analytics

- Decision by the European Data Protection Supervisor - January 5, 2022
  - European Parliament COVID-19 testing website used GA cookies; SCCs.
  - Cookies processed personal data “even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection.”
  - No evidence of transfer impact assessment, supplementary measures.
  - Decision referred to the decision of the Austrian DPA.

Google Analytics

- Formal notice by the French DPA (CNIL) - February 16, 2022
  - Unspecified company using GA; SCCs.
  - Transfers that occur when using GA are “illegal”; similar reasoning to Austrian DPA - Google is subject to FISA 702 and had, in fact, received many such requests.
  - Google’s contractual, organizational, and technical measures to supplement the SCCs were insufficient.
  - Unclear whether there is a way in the interpretation of the CNIL to use GA in a GDPR compliant way.

Google Analytics – Key Takeaways

Privacy+ Security Forum

- Broad interpretation of what constitutes a data transfer: by installing the cookie on the website a data transfer occurred to Google LLC (based in the US) (Austrian DPA)
    - The Austrian DPA noted that the version of GA subject to this case was provided by Google LLC (based in the US) until the end of April 2021. DPA noted that since the end of April 2021, GA has been provided by Google Ireland Limited (based in Ireland).
    - Question: would a data transfer be established in future cases where GA is provided by Ireland?
    - EDPB Guidelines 5/2021 (data importer is located in a third country, without any further specifications) ⇔ Court Case in Germany that ruled that transfer of personal data to US-based cookie provider requires cross-border mechanism under GDPR, even if data never leaves EEA

- Unclear which supplementary measures will be enough to safeguard transfers from the EU to the US
    - Austrian DPA: ruled that in order to be effective, the supplemental measures must eliminate the possibility of surveillance and access to the personal data by U.S. intelligence agencies.
    - EDPS: ruled that the transfers to the US were illegal as the EP did not provide any evidence or documentation on supplementary measures being used on top of the SCCs.

China – PIPL - General

- Personal Information Protection Law (PIPL) went into effect on Nov. 1, 2021
- Key definitions similar to GDPR ("personal information", "processing")
  - "personal information processing entity" → "controller"
  - "entrusted party" → "processor"
- Similar territorial scope, lawful bases for processing, data rights
- Regulator is Cyberspace Administration of China (CAC)
- Robust private right of action

PIPL – Cross-Border Transfer

- Generally requires
  - Notice and consent
  - Personal information protection impact assessment
  - Adoption of protective measures
    - Passing a CAC assessment
    - Certified by a specialized agency
    - Model contract (TBD)
- Data localization for "critical information infrastructure operators"
- Controllers outside of China must carry out data security assessment annually and submit the report to CAC before January 31 each year.
- Draft Measures on Data Export Assessment would require CAC approval for some transfers and require transfer impact assessment for all transfers.

Japan – APPI Amendments

- Amendments to Act on Protection of Personal Information (APPI) go into effect on April 1.
- More detailed notice requirements
  - "must specify the purpose of use in order that the data subject can predict or assume what kind of data processing is being performed"
  - Disclose purpose for using pseudonymized information
  - Joint use disclosures
- Expanded extraterritorial scope – APPI may apply when a foreign business obtains personal information indirectly from a third party
- Clearer breach reporting obligations, expanded data subject rights.

APPI – Cross-Border Transfers

- Exporter must give notice of
  - "personal information protection system" of the importing country;
  - measures taken by importer to protect personal information.
- Under contemporaneous Guidelines, notice should take into account
  - whether the importing country has privacy laws;
  - whether the importing country has obtained GDPR adequacy decision or is a member of Cross-Border Privacy Rules, or any other privacy frameworks;
  - whether the data protection laws and regulations in the country accord with the OECD's Privacy Principles; and
  - other data privacy related rules that would have a serious impact on the data subject's interest.
- U.K. and EEA exempted as PPC has made an adequacy decision.

Upshot – Transfer Impact Assessments

Privacy+ Security Forum

- Know the data and the transfer
  - What data will be transferred?
  - Will there even be a “transfer” under the law?
  - Is the data sensitive or otherwise subject to transfer limitations?
- Know the law
  - What laws in the importing country might impede the transfer?
  - FISA 702
  - EO 12333
  - Rules of civil/criminal procedure
- Know the importing entity
  - Is it subject to invasive laws?
  - Does it have a history of requests/demands?
- Know your options
  - Will supplemental measures mitigate risks?

Parting Thoughts

Parting Thoughts

- Data protection landscape continues to challenge companies and their lawyers
- Prospect for federal privacy legislation appears stalled absent additional states passing comprehensive privacy laws (and subsequent push by corporate interests for consistency)
- Increased scope of regulations and complexity
- Difficult to build a compliance approach due to divergence in legal requirements across jurisdictions and data types
- Regulators are beginning to think about “data issues” together—not just privacy, data security, artificial intelligence, competition, consumer protection, etc. as separate areas of focus

Parting Thoughts

Privacy + Security Forum

- Increasing number of regulators taking an active role in data security and privacy enforcement
- Regulators do not feel that the authority and tools they have are sufficient; stretching what they do have to reach a broader range of conduct
- Investigations are complex, often starting at one place and ending somewhere else entirely
- Importance of "privacy by design" concepts and philosophy—what are you doing, what are you collecting, why, and what are you doing with it
- Smart, thoughtful, reasonable procedures make it less likely a company will face regulatory scrutiny (or at least they present a good defense)
- Anticipate meaningful test cases from FTC, state AGs, and international regulators
- Anticipate "investigations" that are designed primarily to gather information about ongoing practices

Q&A

Privacy+ Security Forum

Speakers

Arianna Evers
Special Counsel
WilmerHale
Arianna.evers@wilmerhale.com

Ali A. Jessani
Senior Associate
WilmerHale
Ali.jessani@wilmerhale.com

Alex Altman
Senior Associate
Arnold & Porter
Alexander.altman@arnoldporter.com