CLS National Conference 2022

Attorney Paul Winters, Wagenmaker & Oberly, LLC

The information provided in this presentation does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this presentation are for general informational purposes only. Participants in this presentation should contact their attorney to obtain advice with respect to any particular legal matter.

1 Global Data Privacy Frameworks

There are two main sets of frameworks for data privacy: US and international.

1.1 International Data Privacy Law – An alphabet soup of legal frameworks

a. GDPR – European Union – General Data Protection Regulation – effective May 25, 2018
b. LGPD – Brazil – effective July 1, 2021. "General Personal Data Protection Law" differs from GDPR, legal basis rights.
c. POPIA – South Africa – Protection of Personal Information Act
d. PIPL – China – Personal Information Protection Law - more to say about this later
e. Many others (South Korea, Australia, Canada, the list goes on)

1.2 GDPR – At present the dominant global framework

a. Broad definitions of "personal data" – any information that relates to an identifiable person. Names, addresses, IP addresses, location, date,
b. Applicable to persons "in" the EU. Ambiguous – employees, residents, visitors
c. Robust provisions for personal control of personal data
d. The fundamental "right to be forgotten" – similar significance as First Amendment rights.
e. Real and active enforcement actions in 2021
    i. € 225,000,000 – 9/2/2021 - WhatsApp Ireland Ltd. – failure to properly disclose user information shared between WhatsApp and related entities (Facebook, Instagram)
    i. € 750,000 – TikTok – 4/9/2021 – failure to provide a Dutch translation of privacy statement
    ii. € 450,000 – Booking.com – 12/10/2020 – failure to timely report a data breach
    iii. € 450,000 – Twitter – 12/15/2020 – failure to meet data breach notification obligations
    iv. € 400,000 – Monsanto – 7/26/2021 – failure to notify data subjects about collected data
    v. € 200,000 – Brussels Airport Zaventem – 4/4/2022 – insufficient legal basis for data processing
    vi. € 1,250,000 – Lisbon City Council – 12/21/2021 – insufficient legal basis for data processing
    vii. €500 – Bar Owner – 5/11/2022 – Non-compliance with general data processing principles

1.2.1 Compliance Applicability – GDPR. Assess organizational participation involving persons in the EEA.

a. Do I have to comply? What must I do to comply?
b. Employees

c. Physical Presence
d. Donors
e. Stakeholders
f. Activities in the EEA, programs, charitable beneficiaries, partner organizations
g. Transfers of Personal Information from the EU to US

1.2.2 Nonprofit Compliance Basics – GDPR

a. Identify organizational data uses. Catalogue process, focus on what's needed.
b. Develop website privacy policy for accurate disclosures (accuracy matters).
c. Don't forget cookies – under EU Cookie Directive, in addition to GDPR.
d. Assign a Data Protection Officer (DPO). Not necessarily a new position.
e. Implement data subject control processes (editing, updating, deleting).
f. Identify and utilize GDPR-approved "derogations" – exceptions (like consent)
    i. Contracts, employment agreements, Partner agreements.
g. Use standard contractual clauses with approved GDPR compliant third parties

1.3 China – Effective August 20, 2021 – Personal Information Protection Law of the People's Republic of China ("PIPL")

1.3.1 PIPL Basic Information – Applies to "Personal Information Processing Entities"

a. Effective November 1, 2021
b. Administered by "CAC" - Cyberspace Administration Committee PRC
c. Many provisions parallel to, or similar to, GDPR provisions
d. Ch. 1 Art. 3: Applicable to entities that
    i. Provide services to natural persons in China
    ii. Assess or analyze activities of natural persons in China
    iii. Are subject to "other circumstances" provided in laws or administrative regulations

1.3.2 PIPL "Personal Information" = broad, perhaps broader than GDPR

a. "All kinds of information"
b. Electronic or otherwise
c. Related to identified or identifiable natural persons *Ch. 1 Art. 4*

1.3.3 PIPL "Personal Information Handling" Definition *Ch. 1 Art. 4*

a. Collection – form fills for newsletters
b. Storage Use – keep it – this might impact records retention
c. Processing – If you don't do the collection but you manipulate or use that data
d. Transmission – sending
e. Provision
f. Disclosure – sharing
g. Deletion – destroying data counts as handling

1.3.4 Personal Information Handling under PIPL *Ch 1. Art 5*

a. Must have a clear, reasonable purpose
b. Must be limited to the smallest scope required to achieve that purpose – if an IP address is not needed to perform your purpose, cannot collect.
c. Must be performed using measures necessary to safeguard Personal Information *Ch. 1 Art. 9*

d. Significant notification requirements concerning processing (at each new use) *Ch. 2. Sec. 1. Art 17*
e. Retention of Personal Information limited to the minimum needed for Personal Information Handling *Ch. 2 Sec. 1 Art. 19*

1.3.5 Conditions for Personal Information Handling (one of the following is required) *Ch. 2 Sec. 1 Art. 13*

a. Obtaining individual consent
b. Contracts with interested individuals
c. Necessary for HR management, labor rules, and collective contracts
d. Statutory duties/obligations
e. Sudden public health incidents, emergency conditions
f. News reporting, public opinion, and activities in the public interest
g. Previously self-disclosed or lawfully disclosed
h. Administrative or regulatory circumstances

1.3.6 Consent under PIPL

a. Must be knowledgeable, voluntary, explicit. Cf. GDPR (also requiring "specific") *Ch. 2 Sec. 1 Art. 14*
b. Must be obtained anew when there are changes in Personal Information Handling *Ch. 2 Sec. 1 Art. 14*
c. May be rescinded *Ch. 2 Sec. 1 Art. 15*
d. Required of parents/guardians of minors under the age of 14 *Ch. 2 Sec. 2 Art. 31*

1.3.7 Sensitive Personal Information *Ch. 2 Sec. 2 Art. 28*

Must adopt strict protection measures. Notification about the handling is necessary and affects interests.

a. "may easily cause harm to the dignity of natural persons or grave harm to personal or property security,"
b. Includes biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc."

1.3.8 China-based representative? *Ch. 5 Art. 53*

a. Entities outside China must establish a dedicated entity or appoint a representative within the borders of the People's Republic of China if they:
    i. provide products or services to natural persons inside PRC;
    ii. analyze or assess activities of natural persons inside PRC; or
    iii. are subject to circumstances provided in other laws or administrative regulations.
b. We don't fully know what this will look like

1.3.9 PIPL - Third Party Handling *Ch. 2 Sec. 1 Arts. 20-21*

a. Like Controller/Processor relationships under GDPR with required third party "entrusting" agreements similar in function to standard contractual clauses
b. Similar daisy-chaining to GDPR, chains of compliance obligations

1.3.10 Conditions for Cross Border Transfers (outside PRC) – must meet one of the following *Ch. 3 Art. 38*

a. Pass a PRC implemented security assessment
b. Undergo a Personal Information protection certification through a PRC-approved provider
c. Utilize standard contractual forms formulated by the PRC. Yet to be released.
d. Other conditions as may be promulgated – administrative regulations and laws

1.3.11 PIPL Individual Rights *Ch. 4 Arts 44 - 50*

Similar to GDPR, rights to:

a. Access, correct, information
b. Erasure/Deletion
c. Explanations Personal Information Handling
d. Object to specific processing
e. Data Portability
f. Withdrawal of consent – importance of CRM audit – keep records
g. Lodge complaints with regulators
h. Lawsuits in the PRC against entities who fail to honor these rights

1.3.12 PIPL Responsibilities

a. Audits of Personal Information Handling *Ch. 5 Art. 54*
b. Personal Information Protection Impacts *Ch. 5 Arts. 55-56*
c. Data Breach Requirements *Ch. 5 Art. 57*

1.3.13 Penalties Ch. 7 Art. 66

a. Level 1 penalties
    i. Organizations < 1 million Yuan ($155,118 USD)
    ii. "Directly responsible personnel" 10,000 – 100,000 Yuan ($1,551 - $15,511 USD)
b. Penalties in circumstances that are "grave"
    i. Organizations < 50 million Yuan ($7,755,906 USD)
    ii. "Directly responsible personnel" 100,000 – 1,000,000 Yuan ($15,511 - $155,118 USD)
c. Possible criminal liability when PRC national interests are at risk

1.3.14 US PIPL Compliance Considerations – Similar to assessment under GDPR – Assess the following

a. Employees
b. Physical Presence
c. Donors
d. Stakeholders
e. Activities in China
f. Transfers of Personal Information from within China to locations external to China

1.3.15 US PIPL Compliance Basics – Be mindful of the recognized conditions for Personal Information Handling

a. Obtaining individual consent
b. Contracts with interested individuals
c. Necessary for HR management, labor rules, and collective contracts

d. Statutory duties/obligations
e. Sudden public health incidents, emergency conditions
f. News reporting, public opinion, and activities in the public interest
g. Previously self-disclosed or lawfully disclosed
h. Administrative or regulatory circumstances

1.3.16 US PIPL Compliance Basics

a. Clearly disclose uses of information through privacy policies and at point of sale/transactions
b. Identify lawful basis for use of data
c. Develop and implement data breach and notification policies
d. Utilize GDPR-like consent, data management and withdrawal mechanisms, i.e., data subject control over personal information
e. Begin to assess possible needs for in country authorized representatives and watch for additional regulations.
f. Get consult on whether large volume data handler conditions apply.

1.3.17 US PIPL Compliance Basics - Stay Tuned

a. The implications of PIPL are not fully understood.
b. Subsequent regulations will be key – stay attentive.

2 US Data Privacy Frameworks

2.1 US Privacy Law – 2021-2022, A year of rapid developments

Backdrop: International privacy law is wholistic, whereas US regulation has been piecemeal, but note many new state and potential federal developments

2.2 Federal Law

a. The FTC Act targets unfair/deceptive commercial practices. *15 U.S.C.A. § 45*
b. GLBA relates to nonpublic personal information by financial institutions. *106 P.L. 102*
c. HIPAA Health Insurance Portability and Accountability Act of 1996 (*104 P.L. 191*), as amended by HITECH (health data) - Health Information Technology for Economic and Clinical Health Act (*42 USCS § 17901* data breach increased fines)
d. COPPA – Children's Online Privacy Protection Act *15 USCS § 6501*
e. CAN-SPAM – Controlling the Assault of Non–Solicited Pornography and Marketing *15 USCS § 7701*
    i. Opt-out provisions, not disguising senders
f. TCPA – Telephone Consumer Protection Act *102 P.L. 243*
    i. Donor outreach - affects things like auto dialers, automated text messages.

2.3 New Pending Federal Law

a. 117th CONGRESS, 2nd Session, HR 8152 - American Data Privacy and Protection Act. The House Committee on Energy and Commerce approved ADPPA on July 20, 2022, ADPPA will be sent to the full U.S. House of Representatives for consideration, and it passes the House to the senate.
b. This would be landmark legislation in this space and would change the amalgam-like approach that currently characterizes U.S. privacy law.
c. Preemption: The Bill contains the following preemption language: "No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation,

rule, standard, requirement, or other provision having the force and effect of law of any State, or political subdivision of a State, covered by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act."

d. Applicability: Any person that "collects, processes, or transfers covered data and is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.)," Also would extend FTC jurisdiction over nonprofit organizations.
e. Possible exemptions:
f. Small data exception. To qualify (1) annual gross revenue below some threshold for each of the prior 3 years, and (2) not process the data of more than 100,000 individuals, and (3) not derive more than 50% of its revenue from transferring covered data.
g. Features:
    i. Data control for consumers (Opt in, Opt out)
    ii. Transparency
    iii. Rights for children under 16
    iv. Data security protocols
    v. Nondiscrimination
    vi. DPOs or equivalents

2.4 Pre-2020 State Laws

a. CCPA – California Consumer Privacy Act - *Cal Civ Code § 1798.199.10*
    i. For-profit focus. This is the front-runner of US privacy law.
    ii. Look for California Rights Privacy Act effective January 1, 2023. Enforcement by AG, new enforcement entity.
b. Massachusetts Data Security Regulation *201 CMR 17.01* (PCI-DSS overlap)
    i. Protection of sensitive data, like SSNs.
c. Maine's Act to Protect the Privacy of Online Consumer Information (ISP regulations) *35-A M.R.S.A. § 9301*
d. Nevada's Online Privacy Laws *Nev. Rev. Stat. Ann. §§ 603A.010* (regulates sharing and sales of personal information)
e. Data breach obligations. All 50 states, varying obligations.

2.5 New State Laws (2021-22): Utah, Colorado, Virginia, Connecticut, and California (again).

a. Utah
b. Colorado
c. Virginia
d. Connecticut.
e. California

2.6 Utah

a. Utah Consumer Privacy Act, U.C.A. 1953 § 13-61-101, *et seq.*
b. Effective: Dec. 31, 2023
c. Scope of application:
    i. Conduct business in Utah or produces a product or service that is targeted to consumers who are residents of Utah; and
    ii. Entities with annual revenue of $25,000,000 or more; and
    iii. Either processes personal data of 100,000 or more consumers; **or** derives over 50% of gross revenue from the sale of personal data and processes personal data of 25,000 or more consumers.
d. Consumer Rights:

i. Right to access.
ii. Right to delete.
iii. Right to data portability.
iv. Right to opt out of certain processing.

e. Obligations:
i. Transparency
ii. Consent to process children's personal data
iii. Security.
iv. Nondiscrimination.
v. Responding to consumer requests.

f. Enforcement
i. No private right of actions.
ii. Through Utah AG.

2.7 Colorado

a. Colorado Privacy Act, C.R.S.A. § 6-1-1301
b. Effective: July 1, 2023
c. Scope of application:
i. Controls or processes the personal data of at least 100,000 consumers or more a year; or
ii. Derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.
iii. No minimum dollar threshold for entities or transactions.

d. Consumer Rights
i. Right of access.
ii. Right to correction.
iii. Right to delete.
iv. Right to data portability.
v. Right to opt out.

e. Obligations
i. Transparency.
ii. Specify purpose.
iii. Data limits and consistent purposes.
iv. Security.
v. Nondiscrimination.
vi. Sensitive data.

vii. Required assessments.

f. Enforcement
i. No private right of action
ii. Enforcement through AG and District Attorneys
iii. Fines according deceptive trade practices - $20,000/violation

2.8 Virginia

a. Consumer Data Protection Act. VA Code Ann. § 59.1-575
b. Effective: January 1, 2023
c. Scope of application:
i. Controls or processes the personal data of at least 100,000 consumers or more a year; or
ii. Controls or processes the personal data of at least 25,000 and derives at least 50% of its gross revenue from the sale of personal data.
iii. No minimum dollar threshold for entities or transactions.

d. Consumer Rights

i. Right of access.
ii. Right to correction.
iii. Right to delete.
iv. Right to data portability.
v. Right to opt out.
vi. Right to appeal.

e. Obligations
i. Specific to purpose for use and collection.
ii. Security.
iii. Required Privacy Policy.
iv. Nondiscrimination
v. Agreements. (GDPR-like)
vi. Required assessments.

f. Enforcement
i. No private right of action
ii. Enforcement through AG
iii. Fines up to $7,500 per violation

2.9 Connecticut

a. An Act Concerning Personal Data Privacy and Online Monitoring, S.B. No. 6, Session Year 2022
b. Effective: July 1, 2023
c. Scope of application:
i. Conduct business in Connecticut, or produce products or services that are targeted to Connecticut residents; and
ii. Controls or processes the personal data of at least 25,000 consumers; and
iii. derives at least 25% of its gross revenue from the sale of personal data.
iv. No minimum dollar threshold for entities or transactions.

d. Consumer Rights
i. Right of access.
ii. Right to correction.
iii. Right to delete.
iv. Right to data portability.
v. Right to opt out.

e. Obligations
i. Specific to purpose for use and collection.
ii. Security.
iii. Transparency/Privacy Policy.
iv. Sensitive Data Opt-In
v. Mechanism for consent revocation.
vi. Nondiscrimination
vii. Special opt-in for children under 16.

f. Enforcement
i. No private right of action
ii. Enforcement through AG
iii. Grace period 1 July 2023, and ending on 31 December 2024 for correction
iv. Penalties in AG's discretion (scope of violation, other factors).

2.10 California

a. 2018 California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100 et seq, was adopted. November, 2020 Proposition 24 – California Privacy Rights Act ("CPRA") amended CCPA.
a. Effective: CPRA January 1, 2023 (but with 12-month look-back).
b. Scope of application:
   i. For-profit organization that "does business" in the state of California; and
   ii. Collects the personal data of Californians; and
   iii. Buys, sells, or shares the personal information of 100,000 people or households, OR. creates 50% or more of your revenue through the sale or sharing of personal information, OR had $25 million in gross revenue in the preceding calendar year.
   iv. "Consumers" includes employees
c. Consumer Rights
   i. Right of access.
   ii. Right to correction.
   iii. Right to delete.
   iv. Right to object to sale or share.
   v. Right to opt-out of behavioral profiling and automated decision-making
   vi. Right to object to the use of sensitive personal information
   vii. Right to data portability
   viii. Right to opt out
d. Obligations
   i. Specific to purpose for use and collection.
   ii. Security.
   iii. Data retention
   iv. Transparency/Privacy Policy.
   v. Sensitive Data Opt-In
   vi. Mechanism for consent revocation.
   vii. Nondiscrimination
   viii. Special rights for children under 16 (consent/treble fines)
   ix. Cookies (if they collect PII) are subject to CPRA.
b. Rulemaking and regulations. By August 2022, there were about 66 pages or proposed rules and regulations.
e. Enforcement
   i. AG has enforcement powers
   ii. Establishes California Privacy Protection Agency, Cal. Civ. Code § 1798.199.10 et seq., enforcement powers here as well.
      i. Establishes a private right of action for certain data breaches: "[u]nauthorized access and disclosure of certain nonencrypted and nonredacted personal information due to a business's failure to "to implement and maintain reasonable security procedures."
      ii. Joint and several liability for administrative fines where "two or more persons are responsible for any violation or violations." Cal. Civ. Code § 1798.199.55(b)
      iii. $2500 per offense, $7500 per offense for willful offenses.
      iv. Significant enforcement action against Sephora for violations of CCPA – September 2022 – $1.2 million.

2.11 Legislation Pending for 2023: Michigan, Ohio, Pennsylvania, and New Jersey

These states' privacy laws are in committee.

2.12 Compliance Basics – US

a. Fully disclose data uses and processes
b. Self-monitor and adhere to disclosed uses and processes
c. Utilize trusted PCI-DSS compliant vendors for financial transactions and handling of other sensitive information, e.g., SSNs. PayPal, ChasePay, Stripe
d. New state level privacy statutes impose GDPR-type obligations.

2.13 Compliance – Data Breach (GDPR and US)

a. Adopt and implement data breach handling and notification policies
b. Observe notice requirements to donors, users, other stakeholders
c. Observe notice requirements to regulators/administrative/executive bodies of state, federal, and possibly, global jurisdictions. Some jurisdictional analysis goes in here.

2.14 Compliance – Minors

a. Evaluate use of organizational website and digital assets by minors, especially those targeting individuals under 16 and 13 (and 14 under PIPL) years of age
b. Obtain appropriate consents where necessary (COPPA, CCPA, PIPL)

2.15 Compliance – CCPA/CPRA

a. Evaluate applicability of "daisy chain" compliance (also GDPR)
    i. Create awareness, disclosures match use, use a CRM, document audit trail for requests.
    ii. Review vendor agreements
b. Assess public relations aspects v. additional compliance burdens
    i. Additional disclosures
    ii. Additional consents pertaining to minors
    iii. Additional data subject control processes