HOT TOPICS IN CYBERSECURITY

October 27, 2022

Mauricio Paez (New York City)
Jeff Kapp (Cleveland)

AGENDA

- Introduction of Risk Trends
- Data Privacy and Security Key Developments
- Health Care Research – HIPAA
- International Data Transfer Developments
- Data Commercialization
- False Claims Act Liability
- Privacy Legislation Update

HIGH RISK

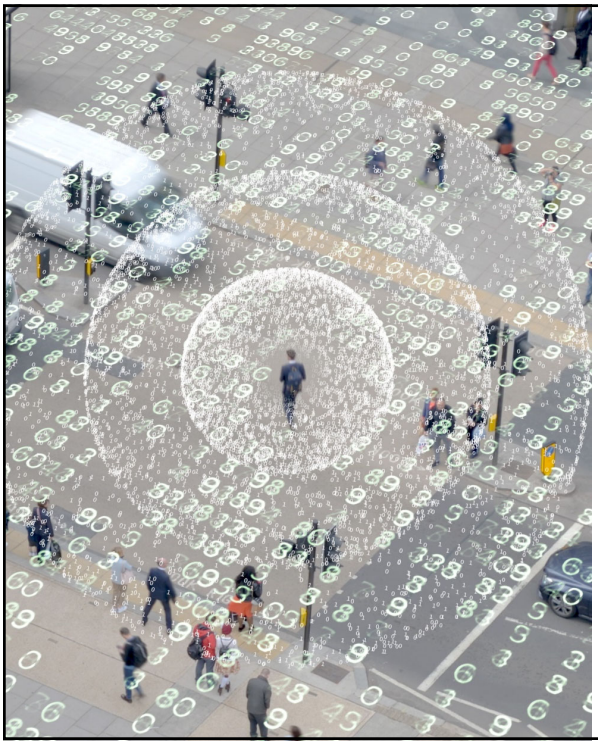
Key Issues

- Ransom and Other Cybersecurity Attacks
- Supplier Risks
- Lack of Privacy Compliance

Key Risks

- Operations Disrupted
- New Breach Notification Challenges
- Legal Risk/Practical Obstacles in Making Ransom Payments
- Heightened Government Involvement/Scrutiny
- Increased Litigation
- Fines by Regulators (e.g., GDPR up to 4 % global turnover)
- Reduced Cyber Insurance Limits

DATA PRIVACY AND SECURITY KEY DEVELOPMENTS



DIGITAL PRIVACY REGULATORY CONSIDERATIONS

- *Dobbs v. Jackson Women's Health Organization*, June 2022
- Fractured state by state approach to privacy
- Renewed regulatory focus on digital privacy:
  - Statements from regulators regarding large-scale consumer data collection: names, contact information, location, zip code, browsing activity on websites or mobile applications
  - FTC: On July 11, warned of intent to use Section 5 authority under FTC Act to investigate unfair or deceptive acts or practices related to transparency of consumer data collection
  - FCC: In July, requested information from top mobile providers regarding data retention and data sharing practices

RECENT ENFORCEMENT ACTIVITY

Regulatory Enforcement	Criminal Investigations	Litigation or Civil Subpoenas
• FTC lawsuit against data broker for selling geolocation data from hundreds of millions of mobile devices • Alleges that the data broker collects and sells geolocation data tied to mobile device ID that could be reidentified in combination with other data • Seeks injunctive relief	• Criminal investigation and arrest of mother and daughter in Nebraska • Subpoena to Meta for private Facebook messages containing medical information	• Third-party data collectors subject to subpoenas for civil enforcement or litigation • Potential consumer litigation over online tracking • Balancing competing factors, including compliance, consumer protection, and brand or reputation

FTC COMMERCIAL SURVEILLANCE & DATA SECURITY RULEMAKING

FTC voted 3-2 to file an Advanced Notice of Proposed Rulemaking on August 11	Citing the heightened risks associated with "[m]ass surveillance," the FTC "is asking the public to weigh in on whether new rules are needed to protect people's privacy and information in the commercial surveillance economy"	Will FTC's actions spur Congress to act? Or create more confusion?	The Commission hosted a public forum on September 8 to discuss the ANPR; public comment period closes on October 21

FTC RULEMAKING AREAS OF FOCUS

Commercial Surveillance Industry Practices

- Collection
- Analysis
- Monetization

TC Concerns

- Lax data security
- Harm to children
- Retaliation
- Surveillance creep
- Inaccuracy

California (CCPA/CPRA)	Virginia (VCDPA)	Colorado (CPA)

• Applies to personnel and business contacts
• Exempts protected health information collected by a covered entity/business associate
• Exempts HIPAA-compliant covered entities
• Exempts PI collected as part of a clinical trial/biomedical research study
• Civil Penalties (Cal. AG) –
  • $2,500 per violation
  • $7,500 per "intentional violation"
	• Does not apply to employees or business contacts
	• Exempts businesses (including companies that must comply with HIPAA and GLBA)
	• Exempts protected health information under HIPAA
	• Exempts clinical trial data
	• Civil Penalties – up to $7,500 per violation (and attorney's fees
		• Does not apply to employees or business contacts
		• Entity-level exemptions (but not for HIPAA-regulated entities)
		• Data-level exemptions (including protected health information)
		• Does not apply to "Private Information" as defined by the Regulations for the Protection for Human Subjects; PI collected as part of human subject research, or Personal Data used in research in accordance with the foregoing two categories
		• Civil Penalties – up to $20,000 per violation

RANGE OF US PRIVACY LAWS (MANY ON EMERGING ISSUES)

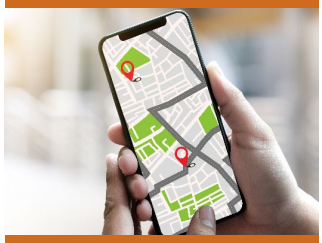
Breach Notification

- All 50 states and U.S. territories (but variance among them)
- New York SHIELD Act

Connected Devices (IoT)

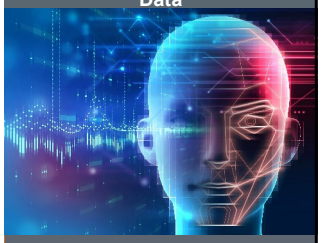
- California and Oregon
- Other states to follow
- Federal law

Data Broker



- Vermont, California, and Nevada*
- Other states and federal law?

Biometric Data & Genetic Data



- Illinois, Texas, and Washington (Biometric)
- California (Genetic)
- Other states following suit

CONNECTED DEVICES – INTERNET OF THINGS

- US State Laws
  - California & Oregon
  - California IoT Act
  - Proposals in 8 other states

- New National Institute of Standards and Technology ("NIST") Proposal for Consumer IoT Product Labeling
- Executive Order directed NIST to initiate two IoT labeling programs
- Key elements of labeling programs, minimum requirements and desirable attributes

- NIST IoT Cybersecurity Standards for IoT
- IoT Device Cybersecurity Guidance for the Federal Government
- Impacts on Internet of Things devices

PROPOSED EU CYBER RESILIENCE ACT

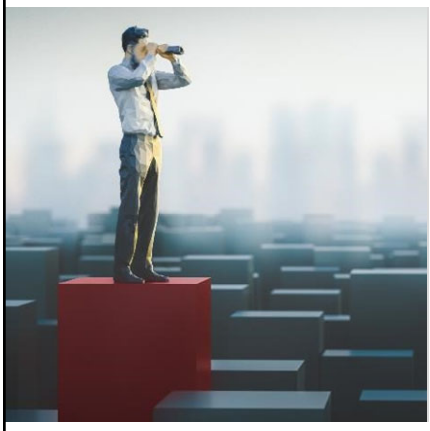
- EU Cyber Resilience Act proposed in September
- Aimed at improving the security of devices
- Products will have to meet various cyber standards to receive approval marking
- Establishes vulnerability database
- Fines: 15 million euros, or 2.5% of a company's worldwide annual revenue

CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

The Act expands and strengthens privacy protections within businesses with online products, services, or features that children under the age of 18 are likely to access

1. Data protection impact assessment
2. High-level privacy default settings
3. Age-appropriate privacy language
4. Clear tracking indicators and geolocation restrictions
5. Additional data privacy restrictions
6. Establishment of a Working Group
7. Specific enforcement and penalties provisions

NEXT STEPS FOR COMPANIES



- Identify types of personal information collected
- Update privacy policies and terms of use for websites and mobile applications
- Implement data retention and minimization
- Limit unnecessary collection of sensitive personal information (e.g., location data)
- Anonymize data before storing, sharing, or selling

HEALTH CARE RESEARCH - HIPAA

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) AND RESEARCH

- Defined: "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge"
- Not covered function under HIPAA (e.g., not Treatment, Payment or Health Care Operations)
- So, research is never a business associate (BA) function

- Researcher might not be a Covered Entity (CE)
- CE if furnishes health care (including to research subjects) and transmits PHI electronically for HIPAA-covered transaction (e.g., billing insurance)
- CE even if third party submits transactions on their behalf

- Researcher might be part of an organization that is a CE
- CE might designate itself as "**hybrid entity**"
- CE can then designate research department as non-covered component since research is not HIPAA function
- But if research department bills insurance, etc., must be part of CE

17 | JONES DAY

HIPAA AUTHORIZATIONS AND RESEARCH

HIPAA vs Common Rule

- HIPAA authorization focused on use and disclosure of PHI
- Common Rule consent is focused on participation in research study as a whole

"Compound" Authorizations

- HIPAA authorizations must generally standalone
- But, can be combined with research study authorization

Conditions

- Generally cannot condition health care, payment, etc., on receipt of authorization
- But, can condition participation in research study on receipt of authorization

18 | JONES DAY

HIPAA RESEARCH EXCEPTIONS

Without Authorization

- Institutional Review Board/Privacy Board Approval
- Preparatory to Research Exception*
- Research on Decedent's Information
- Limited Data Set/Data Use Agreement

With Authorization

- Must meet HIPAA criteria
- Compound authorization permitted
- Condition of participation in study permitted
- May permit use/disclosure for future research

De-Identified Information

- If PHI is properly de-identified, not subject to HIPAA
- BAA may be required if researcher will handle de-identification process

*** Often helpful for study subject recruitment**

INTERNATIONAL DATA TRANSFER DEVELOPMENTS

NEW TRANS-ATLANTIC DATA PRIVACY FRAMEWORK

- 25 March 2022: EU Commission and US agreed "in principle" on new **Trans-Atlantic Data Privacy Framework** ("Privacy Shield 2.0")
- Address CJEU concerns raised in ***Schrems II* decision** – US commitments (to be included in Executive Order) include:
  - **Binding safeguards to limit access to data** by U.S. intelligence authorities to what is necessary and proportionate
  - **New two-tier redress system** to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, includes a "**Data Protection Review Court"**
  - **Strong obligations for companies**, include requirement to **self-certify** adherence to the Principles through the U.S. Department of Commerce
- Likely a 6 months or longer process once the **Executive Order** is published for the European Commission, European Parliament and European Data Protection Board to work out **adequacy decision**

4 MODULES IN SCCS AND FAQS

- **4 June 2021:**
  EU Commission adopted **two sets of SCCs**
  - For the use between **controllers and processors** within the EEA
  - For the **transfer of personal data** to countries outside of the EEA

- **25 May 2022:**
  EU Commission published Q&As to provide **practical guidance on the use of SCCs**
- Helpful **general information** (no legal advice or legally binding character)
- Address **questions** that have come up after publication of the SCCs, mostly for **transfer SCCs**, including:
  - Scope of application
  - Obligations of data exporters and importers under the SCCs (e.g., limitation of liability possible)
  - Governmental access: steps needed to comply with the *Schrems II* decision

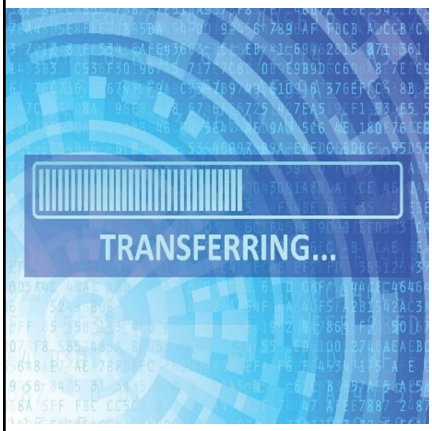
THREE PRONGS OF CHINA'S DATA PRIVACY AND CYBERSECURITY REGIME

Cybersecurity Law 2017	Data Security Law 2021	Personal Information Protection Law 2021
• Imposes cybersecurity obligations to protect national security • Regulates all operators of computer networks (essentially all organizations)	• Imposes data security and localization obligations based on nature of data and national security considerations • Regulates all data handlers	• Imposes GDPR-inspired obligations related to personal information combined with localization obligations • Regulates all handlers of personal information

CROSS-BORDER TRANSFERS OF PI UNDER CHINA'S PIPL

- **Transferring PI out of China requires four elements:**
  (1) informed, voluntary, revocable consent; (2) business necessity; (3) self-assessment of risk, AND (4) one of the following:
  - A CAC security assessment (required for CII Operators and PI Handlers handling or transferring certain volumes of data);
  - A PI protection certification by an organization authorized by CAC;
  - A contract with the foreign recipient based on a CAC standard contractual clause ("SCCs"); or
- **If transferring to a foreign judicial or law enforcement authority, prior government approval required**

CROSS-BORDER TRANSFERS OF PI UNDER CHINA'S PIPL (CONT.)



Recent Developments:

- Guidelines on Security Assessments, effective Sept 1, 2022
  - Mandatory under certain circumstances (data controller processes PI of more than 1 million; previously transferred our PI of >100k or SPI of 10k)
- Guidelines on Certification
  - No authorized certification institutions
- Draft Regulation on SCCs and draft sample SCCs
  - Monitored by PRC authority / notify of a data breach

CHINA PIPL – PENALTIES

Penalties

- Generally not criminal; can be a correction request with provisional suspension
- Up to RMB 50 million ($7.7 million USD) or 5% of previous year's revenue
- Suspend entity's operations or business license
- Private cause of action if an individual's right under PIPL is violated (e.g. right to access, correct, delete)

NEXT STEPS

1. Risk self-assessment (data protection impact assessment with added factors)
2. Update IT policies / employment contracts/ employment manuals -- Consents
3. Understand how business data generated is being automatically stored / duplicated by your IT systems
4. Understand if localization is required
5. Identify the appropriate cross-border data transfer mechanism and mitigation strategy

DATA COMMERCIALIZATION

Corporate Deals	Commercial Deals	Marketing Arrangements

• Not addressing data access needs, protection, and compliance mechanisms early in the deal
• Not understanding the importance of data assets
  • Failure to properly determine importance of data assets and commercialization (pre/post close)
• Not mapping how data will be assessed in terms of their management, protection, and sharing (due diligence, purchase terms, and post closing obligations)
• Not accounting for data commercialization constraints in post-closing / integration
	• Failing to define the data values, sources, and use needs in commercial transactions
	• Not addressing data "ownership" or "property rights" for derivative data
	• Unclear data license rights and sale restrictions
	• Understanding limits of automated processing under data protection laws and evolving AI policies (de-identification/ anonymization)
	• Not accounting for data transfers
	  • Model contracts
	  • Transfer impact assessments
	• Avoiding unclear liabilities and indemnification obligations
		• Not properly defining the regulatory role of the parties (independent/joint controllership, business purpose processing, data processor or service provider, hybrid roles)
		• Failing to address sale and do-not-sell obligations
		• When the marketing arrangement amounts to a data brokerage arrangement, not addressing state registration obligations
		• Not addressing obligations related to cookies and other tracking technologies, use restrictions, and consumer notice and choice obligations

SAMPLE KEY DATA PROTECTION REPRESENTATIONS AND WARRANTIES

DEFINITIONS	Data Protection Laws (DPL), Personal Data/Information, HIPAA, GDPR, Etc.
No Violation of Law	Rep in compliance with DPLs, contractual obligations, authorizations/consents, privacy policies, etc.
No Actions	Rep that there is no action pending, asserted or threatened
Data Protection Measures	Rep that reasonable measures have been taken to protect information against loss, unauthorized access, etc.
Data Breaches	Rep for no data breaches or notifications (including no pending investigations or notices)
Other	Addressing other reps, such as "transaction not breach" and "sale of data"

CLOSING & POST-CLOSING

Closing Covenants/Conditions

- Notice of certain events (e.g., "Seller shall notify Purchaser within X of the occurrence of a Data Breach")
- Cyber insurance (e.g., "Seller shall maintain Cybersecurity Insurance for 3 years with respect to matters occurring prior to Closing")
- Referencing cybersecurity incident(s) in the "no Material Adverse Effect" clause

Post-Closing Issues

- Negotiate ancillary services agreements
- Adjust existing contracts
  - Identify data controllers v. processors
  - Adjust technology arrangements
  - Re-negotiate data use rights
- Implement data transfer mechanisms
- Draft intercompany data sharing arrangements
- Conduct data impact assessments
- Draft required policies, notices and consents

FALSE CLAIMS ACT LIABILITY FOR CYBER MISREPRESENTATIONS: LESSONS FROM *AEROJET*

LIABILITY FOR CYBER MISREPRESENTATIONS

Federal Trade Commission	Department of Justice	SEC
• Consent decrees and ongoing representations to the Agency: Twitter, Facebook, others. • Significant Fines: $5 Billion penalty on Facebook • August 2022: Proposed rulemaking on "commercial surveillance and lax data security"	• *United States ex rel. Brian Markus v. Aerojet Rocketdyne Holdings Inc., et al.* • *Cisco Systems, Inc.* multi-state settlement • October 2021: DOJ Civil Cyber-Fraud Initiative announced	• Pay attention to representations and risk factors in regulatory filings • Proposed Cybersecurity Disclosure Rule • Significant potential enforcement

WHAT'S UP ON THE HILL: PRIVACY LEGISLATION UPDATE

OVERVIEW OF THE ADPPA AND HOW WE GOT HERE

American Data Privacy and Protection Act ("ADPPA") was voted out of committee on July 20, and remains subject to extensive debate in Congress

Will this reconcile the "patchwork quilt" of US privacy laws?

ADPPA comes closest to a viable bill to win bipartisan support, but it is ambitious

Much can still change, including who would be subject to the law, what the law would require, how the law would be enforced, and what laws are preempted by the ADPPA

TWO KEY AREAS OF DEBATE IN ADPPA

Preemption	• Federal laws: GLBA, FCRA, FERPA, or HIPAA? • State laws: CCPA, BIPA, and others?
Private Right of Action	• Private right of action is possible 2-4 years after effective date of ADPPA • But first, individuals must give FTC and their state AG the chance to pursue the matter

CALIFORNIA PRIVACY PROTECTION AGENCY'S RESPONSE

The CPPA called a special meeting in response to the ADPPA after the House Energy and Commerce Committee voted the bill out of committee on July 20

On July 28, the CPPA Board met and voted to oppose the ADPPA and any federal legislation that would preempt or undermine California's privacy protection laws

On September 1, Speaker Pelosi issued a statement implying she would not hold a vote on the bill as currently drafted but that she will continue to work with Chairman Pallone to address California's concerns

QUESTIONS?

Any presentation by a Jones Day lawyer or employee should not be considered or construed as legal advice on any individual matter or circumstance. The contents of this document are intended for general information purposes only and may not be quoted or referred to in any other presentation, publication or proceeding without the prior written consent of Jones Day, which may be given or withheld at Jones Day's discretion. The distribution of this presentation or its content is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of Jones Day.

JONES DAY | One Firm Worldwide®