Data Privacy & Security 2020: *Understanding Enforcement Trends for Strategic Negotiations*

Mehboob R. Dossa
Partner, London
Anne S. Peterson
Counsel, Pittsburgh
Justin T. Yedor
Associate, Los Angeles

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Agenda

- **Introductions:** 5 minutes
- **GDPR Enforcement Trends & Regulator Focus**: 25 minutes
- **CCPA Enforcement Trends & OAG Focus:** 15 minutes
- **New York Division of Financial Services Enforcement Trends & Regulator Focus:** 10 Minutes
- **Questions & Close:** 5 minutes

EU Enforcement Trends & Regulator Focus

- Fines have increased exponentially – UK leading the way!
- Regulator focus is moving from tech companies to other sectors
- Regulators moving from being reactive to proactive
- Causes of enforcement action – cybersecurity and lack of sufficient safeguards, failure to report incidents on a timely basis, lack of lawful basis, cookie consent
- Data subject claims – financial loss and loss of control
- Rise of class actions

Privacy Shield Invalidation

- EU-US Privacy shield – invalid with immediate effect (16th July 2020), there is no grace period.
- SCCs still valid, questionable if they can be used for data transfers to the US. Possibility of new or revised SCCs?
- Localised approach?
- Lack of harmonised approach from EU regulators – sitting on the fence? Certain German DPAs (Berlin, Hamburg and Thuringia) have taken a stronger stance on transfers of personal data to the US using SCCs
- EDPB guidance
- Swiss-US privacy shield –no longer considered adequate by Swiss DPA

Brexit

- UK is now out of EU but GDPR applies, at least for the moment
- Future of data protection co-operation between UK and EU – equivalence, adequacy decision, more BCRs, etc
- UK –US Privacy Shield?
- Lead supervisory authority

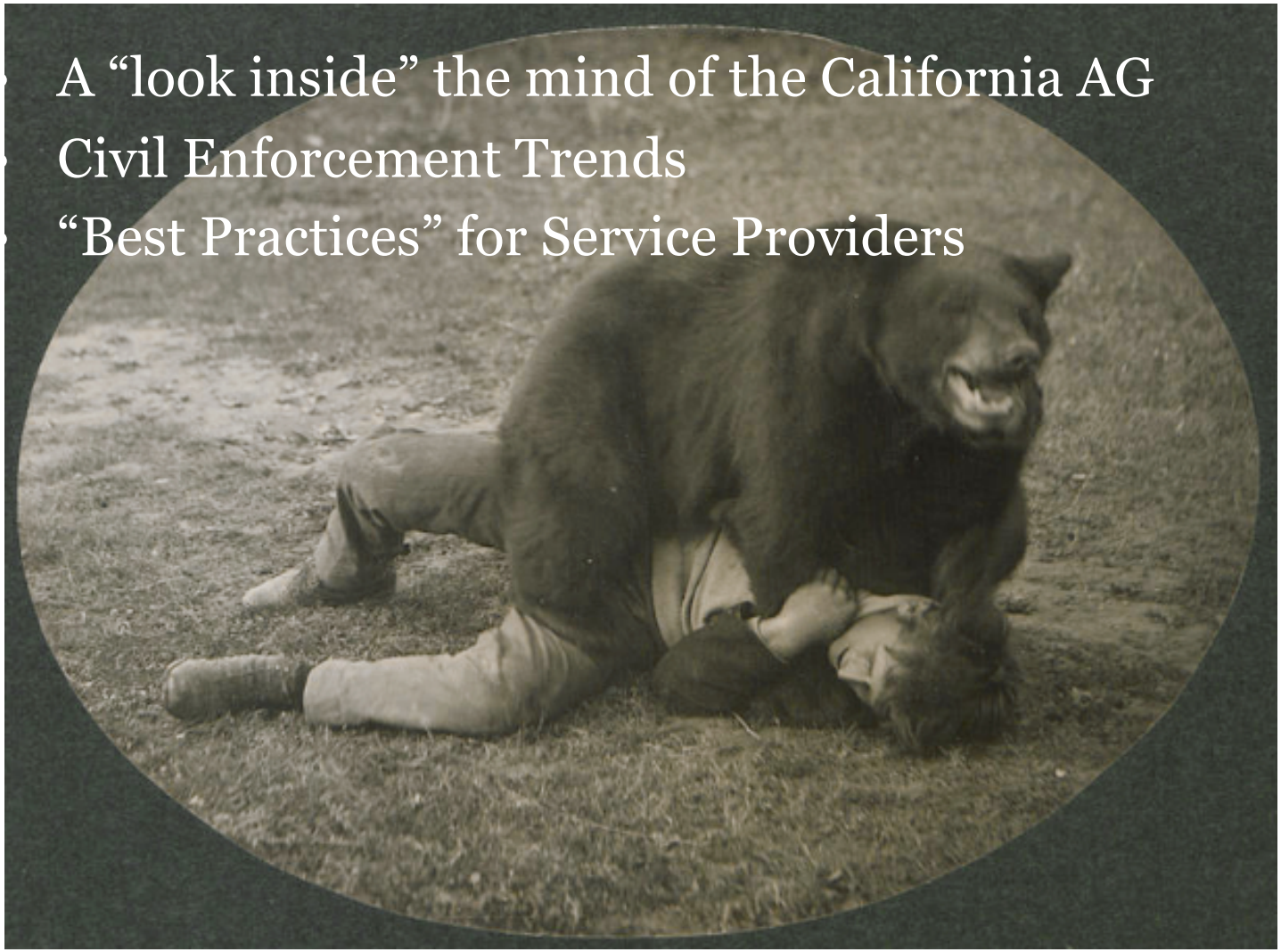
EU Negotiation Strategies

- Use of local/EU service providers or where data will be processed locally
- Minimisation of data transfers and processing
- Due diligence on service providers/M&A target
- Approved code of conduct/industry certification mechanisms for security standards
- Sub-processor approvals

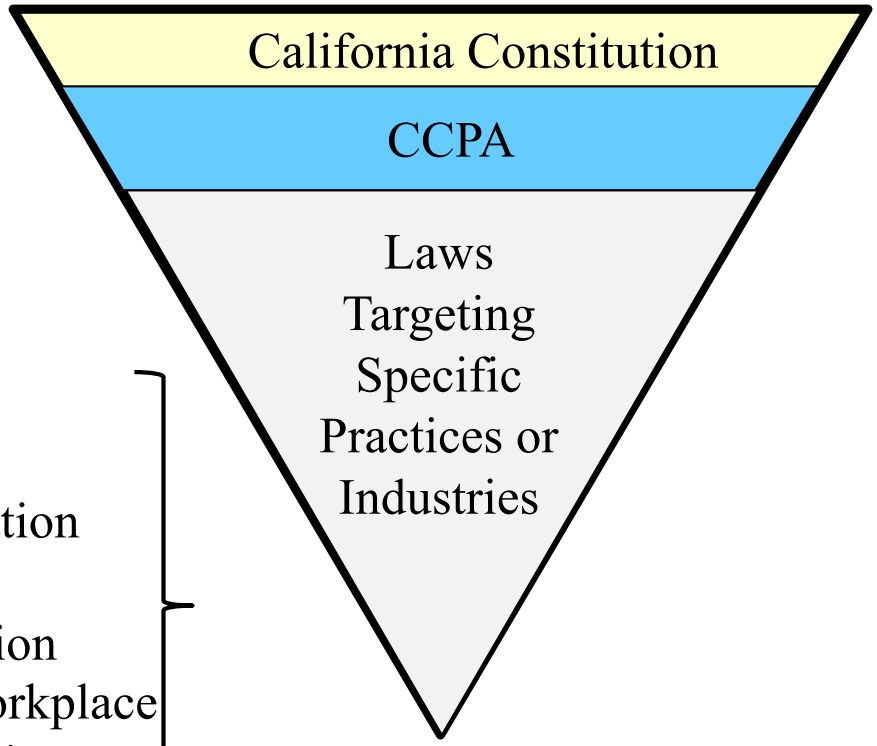
EU Negotiation Strategies (cont.)

- Audit rights
- Specific data protection and security warranties, reps and indemnities (include specific reference to fines)
- Limitation of liability – standard, open ended, super caps
- M&A – Data room set up, structure of the deal, target compliance, target integration, remedial action/condition precedent, transitional data and IT infrastructure sharing

CCPA Enforcement Trends & OAG Focus



The California Privacy Landscape



- Data Disposal
- Data Breaches
- Financial Information
- Credit Reporting
- Medical Information
- Employee and Workplace
- Online/Internet Privacy
- Etc.

CCPA Enforcement Trends – The AG

- Initial letters – July 1, 2020
  - Enforcement limited to the statute
  - BUT, the regulations are now final
- Focused on online-only businesses
- Not limited to any specific industry
- Focused on customer complaints, especially difficulty exercising CCPA rights
- Violations of the rule against "sales" of personal information

CCPA Enforcement Trends – The AG

- Other areas in which the AG has shown interest
  - Children's privacy
  - Sensitive personal information
  - Violations of the CCPA in addition to another statute such as the California Online Privacy Protection Act, the California Confidentiality of Medical Information Act, or the California Unfair Competition Law
  - Repeated consumer complaints
  - Issues raised in class actions that may go unaddressed without AG enforcement
- So far, have not heard of focus on service providers
  - But, service provider relationship is very common
  - Ties into AG's focus on sales

CCPA Enforcement Trends – Civil

- First CCPA class actions filed February 2020
- Dozens of cases filed to date
- Primarily in CA federal courts
- Common claims
  - CCPA
  - UCL
  - CLRA

CCPA Enforcement Trends – Civil

- What is an "unauthorized disclosure"?
  - A data breach? Something else?
- Can unfair trade practices serve as a "back door" for non-data breach claims?

CCPA Enforcement Trends – Civil

What is an "unauthorized disclosure"?

- Cal. Civ. Code § 1798.150 allows consumers to sue when:

  "nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices."

- *Cullen v. Zoom*. Initial Complaint alleged that:

  Plaintiffs' "personal information was subjected to ***unauthorized disclosure*** . . . through the Zoom App where personal information was regularly collected and sent to Facebook and possibly other third parties without authorization."

CCPA Enforcement Trends – Civil

CCPA Enforcement Trends – Civil

Non-Breach Claims Under the UCL

- *Sweeney v. Life on Air*: Direct CCPA claim for failing to provide notice of disclosure of PI to social media
- *Burke v. Clearview AI*: Alleged violation of UCL based on failure to provide notice at or before collection under CCPA
- *Hurvitz v. Zoom, Facebook, LinkedIn*: Similar allegations to *Cullen*, but also alleges that the CCPA violations are a predicate for liability under the UCL
- Will there be others?

CCPA Considerations for Service Providers

CCPA Considerations for Service Providers

- Written contract
  - Disclosure for a business purpose
  - Use PI only for performance of services, to retain subcontractors, for internal quality improvements, for security
  - Agreement not to sell PI – don't forget the "certificate"
- Cooperation between Business and Service Provider
  - How should consumer requests be communicated?
  - Will the service provider process them?
- Indemnity
  - Is mutual indemnity beneficial?
  - Caps on liability?
  - Deferring to the MSA
  - What about data breach insurance as an alternative?

CCPA – Is it still scary?

New York Division of Financial Services Enforcement Trends & Regulator Focus

- July, 2020 NYDFS files ***first*** action enforcing Cybersecurity Regulation against First American Title Insurance Co.
- Multiple violations of Regulation
  - Failure to maintain a cybersecurity program to protect sensitive information
  - Failure senior management failure to approve information security policy and procedures
  - Failure to implement appropriate user access controls
  - Failure to conduct periodic risk assessments
  - Failure to adequately train personnel and update training
  - Failure to implement security controls, particularly encryption, to protect sensitive information

NYDFS Service Provider Requirements

- "Covered Entity "
- Service Providers generally not CEs
- Regulation §500.11 addresses Service Provider obligations
- Requires covered CEs to implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information ("NPI") that are accessible to, or held by, Service Providers
- Mandatory risk assessments
- Documentation of minimum cybersecurity practices required for Service Providers to do business with the CE
- Ongoing due diligence to evaluate the adequacy of Service Provider cybersecurity practices
- Policies and procedures for access controls, encryption, notice of security events

Negotiation Strategies

- Identify customer NPI
- Minimize access/collection/use of NPI for the delivery of services only
- Indemnification and Limitation on Liability should cover all costs related to Service Provider cyber event (fines, sanctions, notification, credit monitoring, all jurisdictions)
- Standard security terms unless particular circumstances require deviations
- Audit, cyber event notification (24 hours), cooperation standard terms
- Standardize risk assessment procedures for Service Provider due diligence
- Documented criteria for evaluating risks and assessing controls

Questions?

Mehboob R. Dossa
Partner, London
+44 20 7632 1627
mdossa@mcguirewoods.com

Justin T. Yedor
Associate, Los Angeles
+1 213 457 9863
jyedor@mcguirewoods.com

Anne S. Peterson
Counsel, Pittsburgh
+1 412 667 7910
aspeterson@mcguirewoods.com