Morgan Lewis

BALANCING DATA PRIVACY OBLIGATIONS AND REGULATORY REPORTING/DISCLOSURE REQUIREMENTS IN INTERNATIONAL EXPORT AND SANCTIONS INVESTIGATIONS

September 15, 2020

Kenneth J. Nunnenkamp
Washington, D.C.

Andrew J. Gray IV
Silicon Valley

Presenters

Kenneth J. Nunnenkamp

Andrew J. Gray IV

Morgan Lewis

Data Privacy and Internal Investigations

- Internal investigations for regulatory reporting
  - Voluntary and mandatory disclosures
  - Internal Investigations
- Data privacy basics
- Conflicts between data privacy and internal investigations/disclosures
  - Meeting privacy restrictions while
    - Satisfying duty of candor and cooperation
    - Managing consents
    - Avoiding material omissions and misrepresentations
- Managing the conflicts; risk allocation

Internal Investigations and Regulatory Reporting; Voluntary and Mandatory Disclosures

- Internal investigations
  - Alternative to government-led investigations
  - Rely heavily on the government's satisfaction that the internal investigation is sufficiently robust and thorough
  - Often require comprehensive reviews once scope is defined
    - Can be broad and sweeping or targeted
  - Provide enough information to allow government agency to decide whether to conduct its own investigation
  - May remain internal or be conducted in conjunction with disclosure to government
  - Form the basis for enforcement decision making by the regulator

Internal Investigations and Regulatory Reporting; Voluntary and Mandatory Disclosures

- Disclosures – voluntary and mandatory
  - Global increase in the use of the disclosure process
    - Voluntary
    - Compelled/Mandatory
    - Coordinated among global agencies
- Common areas for disclosures
  - Anti-money laundering
  - Anti-bribery/anti-corruption
  - Sanctions
  - Export Compliance

Internal Investigations and Regulatory Reporting; Voluntary and Mandatory Disclosures

- Some benefits/impacts of disclosure when done correctly
  - No direct government investigation
  - Likely reduced penalties (enforcement declination)
    - Cooperation credit
  - Improved messaging, internal and external
    - Lead and manage the narrative
    - Employee comfort
    - Management reassurance
  - Measure of control over scoping
    - Types of violations
    - Collection of data
    - Remediation

Data Privacy Basics

- EU and UK as examples
  - General Data Protection Regulation (GDPR)
  - UK Data Protection Act
- Growing number of data protection regimes across the globe
  - China Data Security Law (pending)
  - 132 of 194 recognized nations have some form of data protection law
    - 2/3 have existing laws
    - 10% have draft legislation
    - 20% have no legislation
      - Source: United Nations Conference on Trade and Development (UNCTAD)

Data Privacy Basics

- Data privacy refers to laws that
  - Safeguard individuals' personal data
  - Restrict both where and how such data can be
    - Collected
    - Used
    - Processed
  - Use and processing
    - Broad definition of "processing:
      - any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Privacy Basics

- Establish minimum security standards for sharing
  - Schrem
  - Schrem II
- Impose penalties for unauthorized use
  - Sometime severe
  - Sometimes personal liability as well as organizational
- Require individual consent for uses outside the employment relationship
  - "Consent of the data subject" = freely given, specific, informed and unambiguous indication (i.e., by a statement or by a clear affirmative action), authorizing the processing of their personal data GDPR Art. 4(11)

Data Privacy Basics

- Data privacy laws often require
  - Transparency as to usage
    - Inform the individual *in advance* how personal data is used and processed
  - Data minimization
    - Collection, review and disclosure should be the minimum necessary to achieve the objective
  - Usage only after consent
    - Clearly and in plain language
    - Freely given
    - May be revoked by the individual
  - Collector must have a legitimate reason/interest for processing
  - Certain limited exceptions/exemptions

Conflicts Between Data Privacy and Internal Investigations

- Conflicts arise due to directly conflicting goals and purposes
  - Data privacy focuses on the rights of the individual to privacy and data control
  - Internal investigations and disclosures focus on avoiding a government investigation
- Balance between the competing interests
  - Respecting the contours of data privacy protection while maximizing the impact of the internal investigation and disclosure
  - Explaining the need at the individual level
  - Using special categories correctly
- Dealing with special interests
  - Worker/Works councils
  - Blocking statutes

Managing the Conflicts
Risk Allocation

- Planning ahead
  - Identifying the scope of authorization needed
  - Obtaining consents, where possible
  - Relying on special categories
- Using minimalization to your advantage
- Geographical management of the processing
  - Processing versus transfer
  - Storage of processed data
  - Access to processed data

Managing the Conflicts
Risk Allocation

- Other Legal Bases -- processing
  - Legitimate interest – organization may consider its own legitimate interests, the public interest, or third party interests
    - Requires a balancing of the individual's interests versus the other legitimate interest
    - Alternative tests in the UK
      - Purpose test: is the purpose a legitimate interest
      - Necessity test: is the processing necessary and proportionate
    - Document determinations
    - Consider works council participation and input
    - Collect written consents
    - Third party agreements -- uncertainty after Schrem II

Managing the Conflicts
Risk Allocation

- Use workarounds to address minimalization
  - Process locally
  - Transfer only when absolutely necessary as determined by local and other laws
  - Avoid the "blunderbuss" approach
    - Targeted collections and searches
    - Internal resource assistance
- Vendor management
  - Qualifications and prior experience – understand the difference between doing one project and managing many
  - Controls over the movement of data – consider cyber and encryption issues
  - Vendor agreements compliant with local requirements

Managing the Conflicts
Risk Allocation

- Managing the government disclosure
  - Communicate local restrictions clearly
    - Depending upon the local laws, this could be early/before collection
  - Work with the regulator to manage expectations
    - Some regulators want names, unsanitized emails
    - Determine when and to what extent this is needed
    - Fashion consents accordingly and share the approach with the regulator
  - Enlist the regulator if needed to support authorization via legitimate interest
    - Regulators need names less than often believed
    - Some regulators maintain databases to identify repeat offenders

Managing the Conflicts
Risk Allocation

- Unexpected pitfalls
  - Interviews and interview memoranda that include protected data
    - Personal history
    - Individual protected data
    - Admissions
  - Emails and other communications containing third persons' data
  - Be prepared to address multiple jurisdictions
    - Some jurisdictions acknowledge nationalities
    - Some require the situs rules to apply regardless of nationality
    - Some require work council approvals

Managing the Conflicts
Risk Allocation

- Risk strategies
  - Determine whether the reward for processing and/or transferring merits the action
  - Understand the local penalties for data violations when made in good faith
  - Avoid over-inclusive collection/transfer when not necessary
  - Identify and manage who has access and how
  - Consider redaction for initial provision
    - Use regulator's specific request to support legitimate interest
  - Coordinate if needed with the regulator
  - Use local expertise for consents

Morgan Lewis

Biography

Andrew J. Gray IV
Silicon Valley
+1.650.843.7575
andrew.gray@morganlewis.com

Serving as the leader of Morgan Lewis's semiconductor practice and as a member of the firm's fintech and technology practices, Andrew J. Gray IV concentrates his practice on intellectual property (IP) litigation and prosecution and on strategic IP counseling. Andrew advises both established companies and startups on Blockchain, cryptocurrency, computer, and Internet law issues, financing and transactional matters that involve technology firms, and the sale and licensing of technology. He represents clients in patent, trademark, copyright, and trade secret cases before state and federal trial and appellate courts throughout the United States, before the US Patent and Trademark Office's Patent Trial and Appeal Board, and before the US International Trade Commission.

Biography

Kenneth J. Nunnenkamp
Washington, DC
+1.202.739.5618
kenneth.nunnenkamp@morganlewis.com

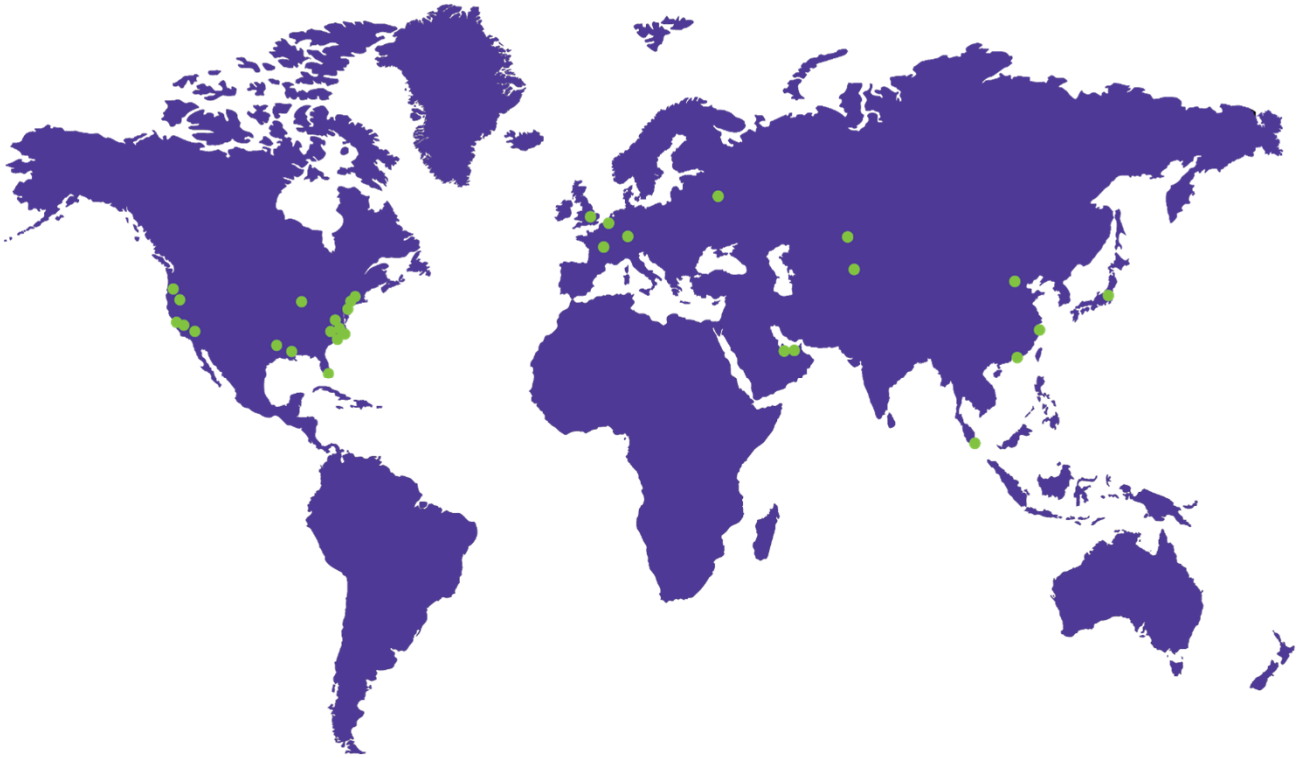
Ken Nunnenkamp represents clients in international trade and national security matters before United States federal courts and government agencies, including the US departments of State, Commerce, Homeland Security, Defense, and Treasury. His practice involves internal investigations and disclosures, including voluntary disclosures and responding to government demands, as well as federal court defense against government actions. He also advises on compliance counseling and training, transactional due diligence–including both domestic and cross-border transactions–and statutory submissions to US government agencies.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU