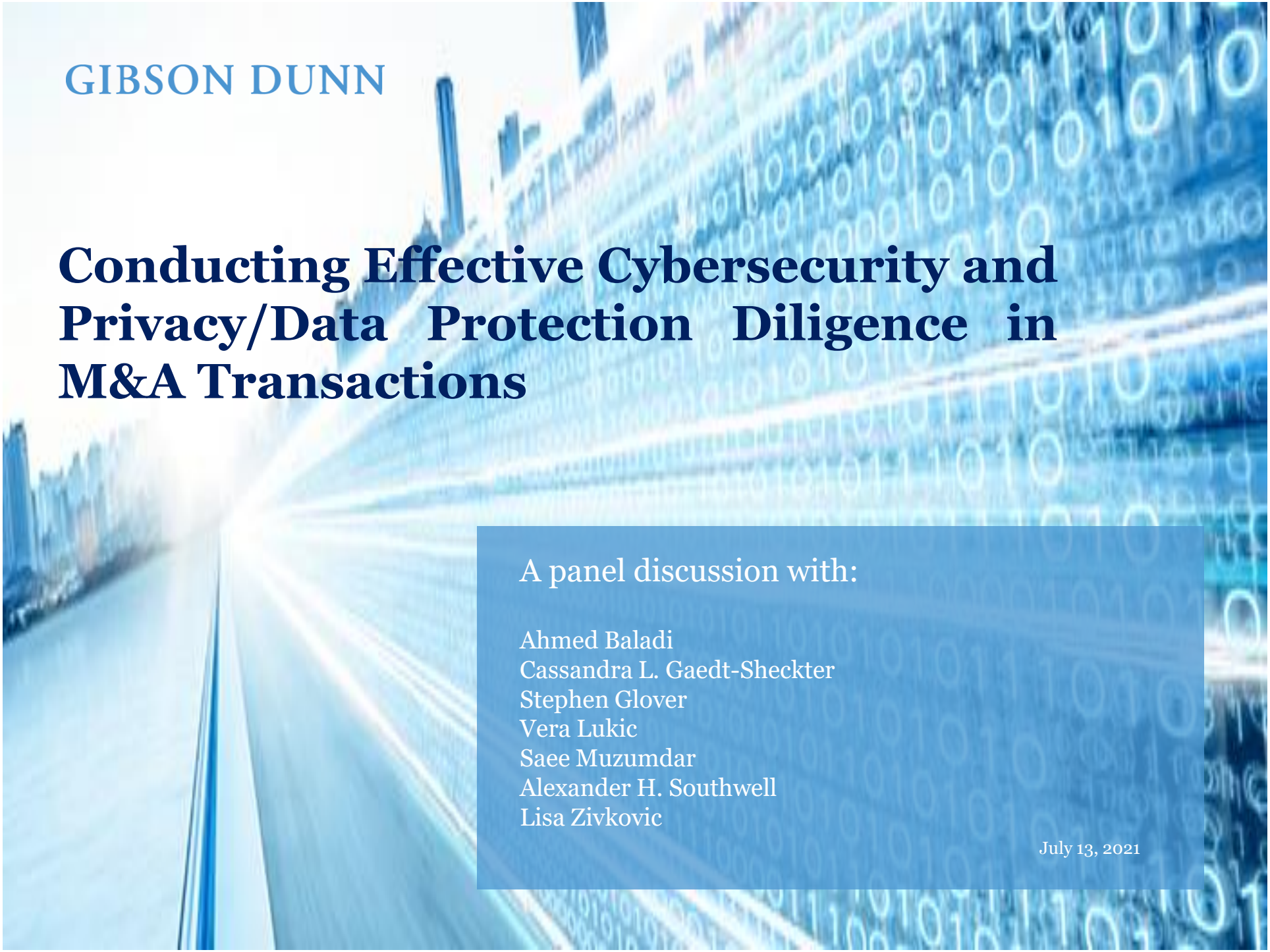


GIBSON DUNN

Conducting Effective Cybersecurity and Privacy/Data Protection Diligence in M&A Transactions

A panel discussion with:

Ahmed Baladi
Cassandra L. Gaedt-Sheckter
Stephen Glover
Vera Lukic
Saee Muzumdar
Alexander H. Southwell
Lisa Zivkovic

July 13, 2021

MCLE Certificate Information

Most participants should anticipate receiving their certificate of attendance via email approximately four weeks following the webcast.

Virginia Bar Association members should anticipate receiving their certificate of attendance eight weeks following the webcast.

Please direct all questions regarding MCLE to CLE@gibsondunn.com

Today's Discussion

1	2	3	4	5	6	7
Introduction	*Overview on the diligence process*	*Focus on US approach*	*Focus on EU approach*	*Other juridictions*	*Assessing and integrating the diligence*	*Deal issues and trends*

Introduction

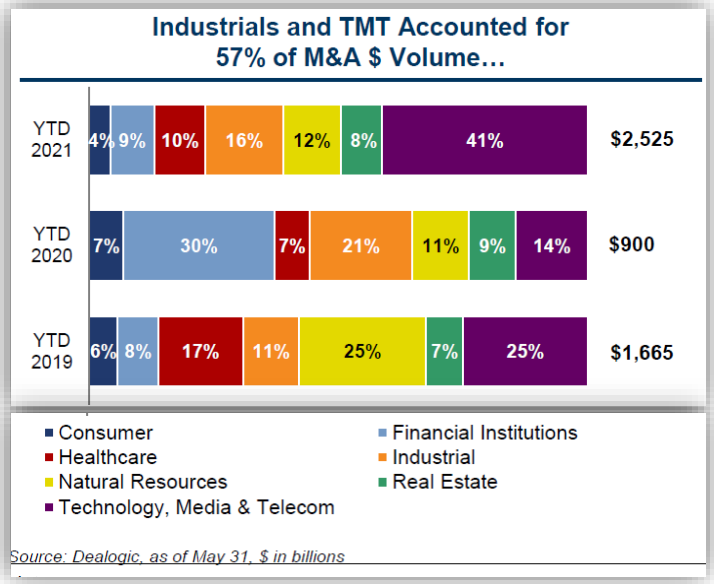
- Managing the cybersecurity and privacy risks associated with M&A transactions has become critical.
- Cyber and privacy regulation is pervasive, and the liability and reputational exposure are significant.
  - There are lots of examples of messy situations in which a buyer has acquired a target's problems.
- The issues are particularly acute in TMT deals, which are a big part of what is driving today's hot markets.
  - But data is important to almost every business, and the problems arise across all industry sectors.
- Transactions with cross-border aspects raise complex issues, because of the need to consider numerous regulatory regimes.

TECHNOLOGY, MEDIA & TELECOM - INNOVATION FEBRUARY 21, 2017 / 1:38 PM / UPDATED 4 YEARS AGO

Verizon, Yahoo agree to lowered $4.48 billion deal following cyber attacks

By Anjali Athavaley, David Shepardson 3 MIN READ

(Reuters) - Verizon Communications Inc VZ.N said on Tuesday it would buy Yahoo Inc's YHOO.O core business for $4.48 billion, lowering its original offer by $350 million in the wake of two massive cyber attacks at the internet company.



Overview on the diligence process

- Takes many forms, particularly depending on sector, size, consumer focus, international reach, and nature and extent of data collected and used.
- Importance of working with internal teams, and using external experts.
- Critical to understand latest trends in regulatory developments and enforcement, US and globally.
- Think about orientation in deal and timeframe.
  - Importance of having checklists ready
  - But also going beyond and digging deeply, if deal considerations warrant
- Data is critical for all companies and may be accessible accross jurisdictions.

Focus on US approach

Penalties & risks under US privacy laws

- CCPA regulatory penalties; up to $7,500 per each intentional violation (or $2,500 for unintentional violation).
- CCPA private action in the event of a data breach; statutory damages of up to $750 per consumer per incident.
- TCPA, CAN-SPAM, BIPA class action lawsuits; statutory damages.
- HIPAA and COPPA penalties of up to $50,000 and $49,792 per violation, respectively.
- Data breach lawsuits; regulator investigations (increased regulatory scrutiny related to cybersecurity).

Focus on US approach

SPECIFIC RED FLAGS	
➢ Lack of awareness of CCPA applicability / requirements and limitation of exemptions (e.g., B2B / employment)	➢ Lack of valid consent / disclosure for collection of health information related to COVID-19 pandemic
➢ Insufficient processes to respond to consumer requests, required contract provisions, disclosure requirements	➢ Insufficient safeguards to protect personal information and company network
➢ Lack of awareness of applicability and requirements of sector-specific privacy and security laws (e.g., HIPAA, COPPA, BIPA, CAN-SPAM, TCPA, FCRA, GLBA, etc.)	➢ Lack of security policies or mere placeholder policies; insufficient incident preparedness, business continuity / disaster recovery plans, and vendor management
➢ Processing of sensitive data (e.g., health data) and/or vulnerable data subjects (e.g., children)	➢ Breach history, issues with response times, security policies not addressing notification requirements (including deadlines)
➢ Varying levels of online policy development: no policy, outdated policy, only online policy, or online policies do not match data collection and processing practices	➢ Past or ongoing claims / investigations

Focus on EU approach

Sanctions & risks under the GDPR

- Up to € 20 million fine (approx. $24 million) or up to 4% of the total worldwide annual turnover of the preceding financial year
- Potential criminal liability in some EU Member States
- Temporary or definitive limitation on processing including on transfers
- Right for individuals to make a complaint (individually or collectively)

Focus on EU approach

SPECIFIC RED FLAGS	
➢ Lack of awareness of GDPR requirements	➢ Insufficient safeguards to transfer personal data outside the EEA
➢ Missing or incomplete GDPR documentation (e.g., record of processing, Data Protection Impact Assessment, Data Processing Agreement)	➢ Lack of valid consent (including for cookies)
➢ Mere implementation of public facing documents	➢ Wrong assessment of the GDPR status (i.e., controller, processor, joint controller)
➢ Processing of sensitive data (e.g., racial, health data) and/or vulnerable data subjects (e.g., children)	➢ Breach history, issues with response times, security policies not addressing notification requirements (including deadlines)
➢ No designation of a lead supervisory authority	➢ Past or ongoing claims / investigations

Other juridictions

Apart from specific US and EU laws and regulations	
Territories	**Laws & Regulations**
APAC	
Australia	Privacy Act No. 119, 1988
China	PRC Cybersecurity Law 2016 - Draft Data Security Law & Personnal Information Protection Law 2021 (PIPL)
Hong Kong	Personal Data (Privacy) Ordinance (Cap. 486) (PDPO)
Japan	Act on Protection of Personal Information (APPI)
India	Information Technology Act 2000 & Personal Data Protection Bill ('the Bill')
Malaysia	Personal Data Protection Act 2010 (PDPA)
South Korea	Personal Information Protection Act 2011 (PIPA)
Singapore	Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA)
Taiwan	Personal Data Protection Act 2010 (PDPA)
America	
Brazil	General Personal Data Protection Law 2018 (*Lei Geral de Proteção de Dados* - LGPD)
Canada	Personal Information Protection and Electronic Documents Act 2000 (PIPEDA)
Europe	
Russia	Federal Law No. 152-FZ on Personal Data
United-Kingdom	Data Protection Act 2018 – UK GDPR

Other juridictions – Focus on APAC

- The data protection landscape in the APAC region is increasingly aligned with the GDPR.
- Australia, New Zealand and Singapore have enacted GDPR-like enhancements, including mandatory data breach notification obligations.
- There is a clear trend towards GDPR-like extra-territoriality and revenue-based fines. China's draft Personal Information Protection Law proposes fines up to 5% of the preceding year's revenue.
- The GDPR is influencing new laws. India's draft Data Protection Bill borrows GDPR concepts such as the right to be forgotten.
- Geopolitical considerations may influence prolific data localization requirements.

Assessing and integrating the diligence

- Post-closing remediation
  - Materiality and priorities
  - Identification of costs and resources needed
  - Consideration of post-closing governance – data privacy and IT experts
  - Integration of the target's privacy and cyber practices into the buyer's global organization
  - Data sharing issues between target and buyer
- Management of specific events
  - Potential cyber incident and/or investigation/claims
  - Impact on the transaction and/or on the business

Deal issues and trends

- Increasing focus on cyber and privacy related diligence
  - Expanded use of internal and external specialists
  - Development of toolkits
  - Early commencement of review process
  - Managing tensions between buyer and seller regarding scope of diligence exercise
- Increasing focus on cyber and privacy related deal documentation
  - Expanded representations
  - Operating covenants and covenants regarding access to information
  - Indemnification coverage
  - Role of representation and warranty insurance and cyber insurance
- Post-acquisition planning and integration

GIBSON DUNN

Questions

Today's Panelists

Ahmed Baladi is a partner in the Paris office and Co-Chair of the firm's Privacy, Cybersecurity and Data Innovation Practice Group. His practice focuses on a wide range of privacy and cybersecurity matters including compliance, investigations and procedures before data protection authorities. He also advises companies and private equity clients in connection with all privacy and cybersecurity aspects of their cross-border M&A transactions.

Alexander H. Southwell is a partner in the New York office and Co-Chair of the firm's Privacy, Cybersecurity and Data Innovation Practice Group. He is a *Chambers*-ranked former federal prosecutor and was named a "Cybersecurity and Data Privacy Trailblazer" by *The National Law Journal*. Mr. Southwell's practice focuses on privacy, information technology, data breach, theft of trade secrets and intellectual property, computer fraud, national security, and network and data security issues, including handling investigations, enforcement defense, and litigation. He regularly advises companies and private equity firms on privacy and cybersecurity diligence and compliance.

Stephen Glover is a partner in the Washington, D.C. office and a member of the firm's Mergers and Acquisitions Practice Group. Mr. Glover has an extensive practice representing public and private companies in complex mergers and acquisitions, including joint ventures, spin-offs and related transactions, as well as other corporate matters. Mr. Glover's clients include large public corporations, emerging growth companies and middle market companies in a wide range of industries. He also advises private equity firms, individual investors and others.

Saee Muzumdar is a partner in the New York office and a member of the firm's Mergers and Acquisitions Practice Group. Ms. Muzumdar is a corporate transactional lawyer whose practice includes representing both strategic companies and private equity clients (including their portfolio companies) in connection with all aspects of their domestic and cross-border M&A activities and general corporate counseling.

Today's Panelists

Cassandra Gaedt-Sheckter is of counsel in the Palo Alto office where her practice focuses on data privacy, cybersecurity and data regulatory litigation, enforcement, transactional, and counseling representations. She has substantial experience advising companies on legal and regulatory compliance, diligence, and risks in transactions, particularly with respect to CCPA and CPRA as one of the leads of the firm's CCPA/CPRA Task Force; GDPR; Children's Online Privacy Protection Rules (COPPA); and other federal and state laws and regulations.

Vera Lukic is of counsel in the Paris office where her practice focuses on a broad range of privacy and cybersecurity matters, including assisting clients with multinational operations on their global privacy compliance programs, cross-border data transfers and data security issues, as well as representing clients in investigations, enforcement actions and litigation before the French data protection authority and administrative courts. She also regularly advises on data privacy aspects of M&A transactions, including with respect to carve-out and transition issues.

Lisa Zivkovic, Ph.D is an associate in the New York Office. She is a member of the Firm's Privacy, Cybersecurity and Data Innovation, Technology Transactions, and Litigation practices groups. Ms. Zivkovic's doctorate is a comparative history of data privacy in the US and European Union. She advises a wide range of clients, including technology, financial services, data aggregation and analytics, vehicle, and telematics companies, on new and complex legal and policy issues regarding global data privacy, cybersecurity, artificial intelligence, Internet of Things, and big data.