The Sedona Conference Journal

Volume 20 2019

The Sedona Conference Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice

The Sedona Conference

Recommended Citation:

The Sedona Conference, *Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice*, 20 SEDONA CONF. J. 233 (2019).

For this and additional publications see: https://thesedonaconference.org/publications

THE SEDONA CONFERENCE COMMENTARY ON DATA PRIVACY AND SECURITY ISSUES IN MERGERS & ACQUISITIONS PRACTICE

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Drafting Team Leader:

Sara Romine

Drafting Team:

Jay Brudz
Craig Carpenter
Cordero Delgadillo
Charlyn Ho
Daniel Meyers
Dana Post
John J. Rosenthal
Jeffrey C. Sharer
James A. Sherer

Steering Committee Liaison:

David Moncure

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference's Working Group 11. They do not necessarily represent the views of any of the individual participants or their

employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors; whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice,* 20 SEDONA CONF. J. 233 (2019).

PREFACE

Welcome to the final, May 2019 version of The Sedona Conference *Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice*, a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This final version of the *Commentary* supersedes the public comment version published in May 2018. This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The Sedona Conference acknowledges Drafting Team Leader Sara Romine for her leadership and commitment to the project. We also thank drafting team members Jay Brudz, Craig Carpenter, Cordero Delgadillo, Charlyn Ho, Daniel Meyers, Dana Post, John Rosenthal, Jeff Sharer, and James Sherer for their efforts and commitments in time and attention to this project. We thank Anand Shah and Maria Garrett for their assistance. Finally, we thank David Moncure for his guidance and input as the WG11 Steering Committee Liaison to the drafting team.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of this *Commentary* were the subject of dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
May 2019

FOREWORD

In the ordinary course of business, companies acquire, use, and disseminate vast amounts of data. This data can provide a company with a competitive advantage, be instrumental to a company's day-to-day operations, or serve no tangible purpose at all. For these reasons, the information possessed by a company can have a range of values but be accompanied by varying degrees of risk depending upon the security of the data and whether its use or dissemination triggers any privacy concerns. Consequently, data privacy and security issues must be considered in an acquisition, and can have a significant impact on the value and terms of the deal, including whether or not to acquire certain data as part of the transaction and how to value that data.

Perhaps the most prominent example of the impact that privacy and security issues can have on a deal is Verizon's contemplated acquisition of Yahoo. After Verizon and Yahoo reached an agreement by which Verizon would acquire Yahoo's core internet operations, it was revealed that Yahoo had suffered two large data breaches impacting more than one billion customers.[1] Verizon and Yahoo delayed the acquisition to assess the impact of the data breaches on the terms of the deal, including the purchase price.[2] Ultimately, in response to pressure from Verizon, Yahoo reportedly agreed to lower the purchase price by

1. Greg Roumeliotis & Jessica Toonkel, *Yahoo Under Scrutiny After Latest Hack, Verizon Seeks New Deal Terms*, REUTERS (Dec. 15, 2016, 9:38 A.M.), http://www.reuters.com/article/us-yahoo-cyber-idUSKBN14420S.

2. Thomas Gryta & Deepa Seetharaman, *Verizon Puts Yahoo on Notice After Data Breach*, WALL ST. J. (Oct. 13, 2016, 7:28 P.M.), https://www.wsj.com/articles/verizon-sees-yahoo-data-breach-as-material-to-takeover-1476386718.

approximately $350 million.[3] The Yahoo example demonstrates the significant impact that privacy and security issues can have on a deal. For this reason, the Yahoo deal is referenced at various points in this *Commentary* as an example. These issues, however, are not limited to high profile "mega deals." Privacy and security concerns exist in virtually every deal.

This *Commentary* is intended to provide practical guidance on data privacy and security issues that must be considered in a potential acquisition. In doing so, it approaches these issues from the perspective of the buyer. It is not intended to be exhaustive, but rather to provide a framework for addressing the privacy and security issues that likely will impact a transaction. Although the title of this *Commentary* refers to "Mergers & Acquisitions" (because such terms are almost always used in tandem to describe a particular area of law practice), the *Commentary* focuses exclusively on acquisitions because true corporate statutory mergers of unrelated entities are increasingly rare.

3. Brian Womack, *Verizon Suggested Price Cut of Up to $925 Million for Yahoo Deal*, BLOOMBERG (Mar. 13, 2017, 12:46 P.M.), https://www.bloomberg.com/news/articles/2017-03-13/verizon-suggested-price-cut-of-up-to-925-million-for-yahoo-deal.

TABLE OF CONTENTS

I. INTRODUCTION 242
II. STAGE ONE: DETERMINING WHAT THE BUYER WANTS TO ACQUIRE AND NEGOTIATING APPROPRIATE DEAL TERMS 244
A. Identifying and Assessing the Different Types of Data That Will Be Acquired 244
B. The Scope, Ownership, and Transferability of the Data Being Acquired 246
C. Subjects of Disclosure, Representation, or Warranty 247
1. Compliance with Data Privacy Laws, Regulations, Industry Standards, and Privacy Policies 247
2. Disclosure of Known or Potential Data Compliance-Related Incidents 248
3. Information Security Representations 249
4. Cyber Insurance 250
5. Export Control 250
D. Stage One Summary 250
III. STAGE TWO: PERFORMING DUE DILIGENCE 252
A. Data Privacy and Security in Acquisition Due Diligence 252
B. Considerations in Conducting Data Privacy and Security Due Diligence 254
1. Due Diligence on Data Privacy and Security Issues Should Not Run Afoul of Prohibitions on "Gun-Jumping" 254
2. Deal Considerations 255

3. Existence of and Implementation of Data-Classification Policies and Related Security Measures 267
4. Business Critical Functions 269
5. Due Diligence Beyond the Data Room 270
C. Adapting the Due-Diligence Process to the Changing Terms of the Deal or Information Being Provided 271
D. Stage Two Summary 272
IV. STAGE THREE: CLOSING AND POST-CLOSING CONSIDERATIONS 275
A. Mechanisms for Allocating Information-Related Risks 276
1. Purchase-Price Adjustments 276
2. Indemnification 277
B. Post-Closing Operational Issues 278
1. Identification and Confirmation of Data Transferred 278
2. Segregation of Data 279
3. Right to Use and Transfer Data 280
4. Contractual Restrictions 280
5. Statutory and Regulatory Restrictions 281
6. Data Separation 282
7. Deletion of Data 284
C. Best Practices for Data Integration 284
1. Summarizing Limitations and Permissions 285
2. Leveraging Institutional Knowledge 285
3. Integration Meetings and Training 286
4. Updating, Adapting, or Revising Policies and Procedures 286

5. Developing a Data-Transition Plan 287
6. Knowing When Not to Integrate 287
7. Recognizing Opportunities for Improvement and Advancement 288
D. Stage Three Summary 289
APPENDIX A: DIFFERENT CATEGORIES AND TYPES OF DATA IMPLICATED IN THE DEAL ANAYLSIS 291
APPENDIX B: SAMPLE REPRESENTATIONS AND WARRANTIES 315
APPENDIX C: DUE-DILIGENCE REQUESTS 330

I. INTRODUCTION

"Information is crucial to modern businesses. Information can have great value, but also pose great risk, and its governance should not be an incidental consideration."[4] This is no less true in an acquisition, where the impact of information on the deal is multifaceted. First, the target company or asset has its own (often unique) data privacy and security issues that may affect the inherent value of the target. Second, the security of sensitive information shared during the due-diligence phase must be ensured because of the possibility of data breach. Third, post-deal integration activities—both strategic and logistical—may hinge on data privacy and security issues, forcing the buyer to change its business strategy or even its operations to accommodate unforeseen issues.

This *Commentary* approaches these issues through the lens of the typical "deal framework" and is thus divided into the three basic stages of a transaction: (i) determining the scope of the acquisition; (ii) conducting due diligence; and (iii) closing and post-closing considerations. At the end of each stage, there is a short summary containing the key "takeaway" points. In addition, the *Commentary* aims to give practical demonstrations of those processes, including sufficient background information to demonstrate how the *Commentary*'s proposed guidance will work in the real world. Given this approach, the *Commentary* is not intended to be exhaustive and certainly could not be—the scope of the issues that may arise will necessarily turn on the specifics of a given transaction and the terms negotiated by the buyer and the seller.

It is our hope that the *Commentary* will be of use not only to professionals working on an acquisition, but also to those

4. The Sedona Conference, *Commentary on Information Governance*, 15 SEDONA CONF. J. 125, 130 (2014).

individuals who will work on the post-deal integration of the acquired assets. In an effort to distill the scope of our analysis into a more practical form, we have also appended to this *Commentary* a summary of the categories and types of data implicated in the deal analysis (Appendix A); sample representations and warranties that address privacy and security concerns (Appendix B); and basic due-diligence requests (Appendix C). Of course, this work product is simply a starting point for analysis and will need to be tailored to each specific transaction.

II. STAGE ONE: DETERMINING WHAT THE BUYER WANTS TO ACQUIRE AND NEGOTIATING APPROPRIATE DEAL TERMS

A. Identifying and Assessing the Different Types of Data That Will Be Acquired

Advancements in computer processing have empowered companies to amass and control data at a faster pace, in larger quantities, and of a greater variety. This reality makes the valuation of risks and benefits associated with such data increasingly difficult. Consequently, the context of data (how and where it was created), the content of data (what information it contains), and the rules that may apply to such data (internal and external policies, court decisions, federal laws, state laws, and regulations) can seem overwhelming. Complicating matters, "new" types of data and novel uses of "old" data may lead to the enforcement or application of arcane and ill-suited rules. Likewise, the ability of the buyer to unlock the potential value of the target's data can be greatly impacted by the nature and type of data systems involved. Thus, in an analysis of an impending acquisition, classification of the target's data is vital to calculating its related value and risk.

Any analysis of an impending acquisition should include a data-classification framework to assist the buyer in determining whether to "take it" or "leave it" as it relates to particular types of data. Data governance models frequently use complex data-classification systems. These systems offer value by automating compliance requirements based on classification. Data classification for an acquisition analysis, however, should remain as simple as possible without impeding effectiveness.

At its most basic level, buyers use data classification to answer two threshold questions: (i) what exactly is the data; and (ii) what value, obligations, and risks accompany it? Data classification is not straightforward, and classes of data often

overlap. It is critical for buyers to think through data classification at the outset, determining how differences in types of data and the regulation of that type of data will account for differences in the classification system. Appendix A of this Commentary sets forth and describes the different categories of data that parties to an acquisition may wish to use as a classification starting point. In addition to these categories of data, Appendix A sets forth particular types of data that are subject to certain laws and regulations that require heightened privacy and security practices (and are subject to regulations or industry group best practices that can be binding on industry members or simply provide guidance). After the parties to the transaction categorize the data subject to the transaction, they should determine whether such data categories trigger special protections. Due to the constantly evolving global regulatory landscape governing data privacy and security, the buyer should consider Appendix A as just one resource to consult when assessing the protections and obligations applicable to the relevant data categories.[5]

Determining whether a company complies with its privacy policies is crucial. Costly enforcement actions can result from a company's failure to follow its consumer-facing privacy policies.[6] Parties to an acquisition must also consider the particular

5. Additional resources include The Sedona Conference, *Data Privacy Primer*, 19 SEDONA CONF. J. 273 (2018).

6. Parties should consider: (i) the type of data collected; (ii) how the data is used; (iii) the target company's policies and third-party agreements relating to such information; and (iv) whether the target company complies with its consumer-facing policies. *See, e.g.*, The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, THE SEDONA CONFERENCE (Jan. 2017), https://thesedonaconference.org/publication/International_Litigation_Principles. In 2014, when Facebook acquired WhatsApp, the Federal Trade Commission and European data protection authorities warned the companies that the parties' failure to abide by WhatsApp's privacy notice would constitute a deceptive act under

treatment of data that enters and exits a country because of export controls[7] and cross-border data protection concerns. Because legal requirements vary at the international, federal, and state levels, analysis requires a data-, industry-, and jurisdiction-specific assessment.

The point of this analysis is to determine the values and risks associated with data that are a necessary part of the acquisition and, for other data, whether to acquire it or leave it behind.

B. The Scope, Ownership, and Transferability of the Data Being Acquired

Fundamentally, a party cannot sell more than it owns. For this reason, after identifying the data that is subject to the acquisition, the parties should specify the extent of the transferor's rights to the data. Ownership may be unclear. Cloud and software-as-a-service (SaaS) storage platforms, employee or customer information in the possession of corporations, and shared intellectual property often preclude up-front ownership analysis. Accordingly, contractual terms, privacy policies, and applicable regulatory regimes should be analyzed to accurately understand and document precisely what rights of ownership or access to relevant data the seller possesses.

Even though the seller has rights to obtain, possess, and use data, the seller may not be able to transfer all of those rights. Buyers must recognize constraints on data transferability, particularly when the deal is structured as an asset sale. Such constraints will often be in the form of pre-existing contractual restrictions found in the seller's existing privacy policies or

---

the Federal Trade Commission Act and European data protection and privacy laws. *See In re: WhatsApp*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/internet/ftc/whatsapp/ (last visited May 9, 2019); Agency Information Collection Activities, 80 Fed. Reg. 2423 (Jan. 16, 2015).

7. *See, e.g.*, BIS Export Administration Regulations, 15 C.F.R. §§ 730–774.

contracts. Diligent buyers should extensively review any such policies to avoid any data transferability issues or limitations that may exist following the acquisition.

C. Subjects of Disclosure, Representation, or Warranty

After assessing and determining the data that will be acquired, the buyer should consider the representations and warranties from the seller that the buyer needs to ensure receipt of its anticipated acquisition and to allocate risk appropriately. Some sample representations and warranties are provided in Appendix B. The following are important matters on which the buyer will want to receive representations from the seller.

1. Compliance with Data Privacy Laws, Regulations, Industry Standards, and Privacy Policies

Privacy regimes are comprised of a complex web of intersecting laws, regulations, and industry standards.[8] Historically, buyers spent little time focusing on the seller's record and information management practices and privacy concerns related to the data being sold. Buyers would frequently obtain all of the seller's data "just in case." Notwithstanding the costs associated with storage and retrieval of this data, utilizing these historic practices subjected buyers to unnecessary legal, regulatory, and business risks.

8. For example, a Massachusetts healthcare company that accepts credit card payments may be required to comply with the privacy norms embodied in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Massachusetts breach notification and information security laws, Payment Card Industry (PCI) standards, and the Federal Trade Commission Act's prohibition against fair or deceptive trade practices. Failure to comply with any of these requirements can result in heavy fines, decreased operational capabilities, and severe reputational and business issues.

While some companies operating within this complex framework have invested the time and resources required for compliance with each applicable norm, others have not. A third party looking to acquire a company—and, in particular, a company that operates in an unfamiliar industry or regulatory environment—faces an uphill battle to understand the applicable privacy regime, let alone measure the target company's compliance with it.

Accordingly, the deal documents should: (i) identify which legal and industry-based privacy norms apply to the target company's business; (ii) identify the contours of the target company's current and prior privacy statements and policies (including any policies that limit the target company's ability to transfer or sell personal information to third parties); and (iii) represent the extent to which the target company is currently in compliance with the two prior points. Additional consideration should also be given to the target company's historical compliance with industry-based privacy norms. Buyers will often require the target company to represent that its business has been in compliance with applicable privacy rules and regulations for a certain look-back period. The parties should also consider whether to include privacy-specific indemnification provisions in the documents to protect the buyer against any variances from the seller's representations. In sum, buyers today are encouraged to vet properly any compliance-related issues throughout the due-diligence process well before closing.

2. Disclosure of Known or Potential Data Compliance-Related Incidents

The representations in the acquisition documents should include disclosures of the target company's known or potential compliance-related incidents, including: (i) contractual violations relating to the use or storage of data; (ii) pending or current investigations relating to data privacy and information

security; and (iii) data-breach incidents or threats, including whether there were any private or regulatory actions taken in response to such incidents. These disclosures can include what actions were taken in response to data-breach incidents in order to comply with state and federal breach notification laws and any related privacy complaints, litigations, enforcement actions, consent decrees, or remediation activities. To the extent an issue is identified during the due-diligence period, the parties may wish to include special indemnities in the purchase agreement to address any associated risks. For additional discussion on indemnities, see Section IV(C).

3. Information Security Representations

Data privacy and information security are related but distinct fields. It is important to consider the inclusion of representations concerning the target company's information security programs and infrastructure. For companies with a robust written information security program, such representations can be accomplished by attaching a copy of the written policy to the acquisition documents and including a representation that the target company is in compliance with the requirements and provisions of that policy.

For companies that lack a pre-existing written information security program, additional due diligence may be required, or the seller may be required to provide a more detailed description of its security apparatus. This description should include the physical, administrative, and technical safeguards the target company has implemented to protect its data from unauthorized access. Those safeguards may include: (i) data access controls; (ii) use of encryption; (iii) Bring Your Own Device (BYOD) or Corporate-Owned Personally Enabled policies; (iv) disaster-recovery and data-backup procedures; (v) corporate training programs; and (vi) the existence of any incident response plans.

4. Cyber Insurance

The parties should also consider whether the target company has insurance policies that provide coverage for the buyer against data privacy or security incidents. This inquiry can be accomplished in the due-diligence process or through representations. If the latter process is chosen, the representation should include coverage limits (per incident and in aggregate) and what third-party services are covered.

5. Export Control

For companies that export goods or services across borders, the parties should consider whether to include: (i) a list of the countries to which the exports occur, and (ii) a representation and warranty that all applicable export licenses have been obtained for each applicable country. These concerns can also be addressed during due diligence as a supplement to or replacement of such representations.

D. Stage One Summary

During the initial stage of the acquisition, the buyer should:

- identify specific types of data to be acquired and assess the information governance requirements and the risks associated therewith;
- determine the scope, ownership, and transferability of the data being acquired, including any contractual or common-law restrictions on the sale or transfer of the data;
- assess the target company's current compliance with any applicable data privacy laws, regulations, industry standards, and the target company's own privacy policies;
- obtain disclosures of any known or potential data compliance-related incidents, including

any data-breach incidents and legal actions taken against the target company;

- procure representations and warranties concerning the target company's information security program and infrastructure, including by appending any applicable policies and obtaining representations that the target company is currently in compliance with all such policies;
- determine the existence of any cyber insurance policies; and
- obtain disclosure of any countries to which the target company provides goods and services, and obtain representations and warranties that all necessary export licenses have been acquired.

III. STAGE TWO: PERFORMING DUE DILIGENCE

A. Data Privacy and Security in Acquisition Due Diligence

A well-informed buyer is more likely to achieve its goals for an acquisition. Accordingly, pre-signing due diligence is an integral part of the deal-making process. The success of the transaction relies upon reducing the risks associated with both the transaction and the post-transaction going concern and justifying the costs paid and strategy envisioned in the transaction.[9]

Traditional due diligence is used to determine the liabilities, efficiencies, and price of a proposed transaction. Due diligence often provides insight into whether the buyer should proceed with a given deal and whether the deal value should be adjusted. A buyer uses the diligence process to determine whether there are any incompatibilities that could not be identified based on public information. Traditional mergers and acquisitions (M&A) diligence typically is useful in identifying "red flags" or unanticipated liabilities not covered by representations and warranties relating to:

- assets (tangible and intangible);
- organization;
- contracts;
- customers;
- employment information;
- environmental issues;
- finances;
- litigation profile;
- suppliers and distributors; and

9. James A. Sherer et al., *Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, e-Discovery, and Information Governance into Due Diligence Practices*, 21 RICH. J.L. & TECH. 5 (2015).

- tax issues.

Recently, data privacy and security have become important subjects of diligence. This trend is driven in significant part by burgeoning legal implications. A changing regulatory landscape has increased the risk associated with unknown data privacy and security practices.[10] Responses to these regulations are complex as well, and many organizations are struggling to keep up. Under such circumstances, buyers may be better served assuming an environment of noncompliance for targets, and therefore working to determine an appropriate risk analysis for post-transaction activities.[11]

Proper data privacy and security diligence can aid in demonstrating the maturity level of the target with respect to: (i) data privacy and security issues; (ii) determining greater cost certainty for the transaction; (iii) identifying integration or migration issues early in the transaction; and (iv) decreasing the buyer's risk.[12]

As discussed in more detail below, data privacy and security diligence in an acquisition should, at a minimum, consider: (i) the type of sensitive information involved; (ii) the location of sensitive information; (iii) the target's current and historic data security and privacy practices; (iv) known vulnerabilities and breaches; and (v) the target's relationship with vendors. This information is imperative for the buyer to be able to understand and assess the risks of liability associated with the target company. This information must be requested and reviewed by someone who understands the business and legal implications stemming from the acquired information. Therefore, the parties should each establish a transaction "quarterback" to serve as the

10. *Id*.

11. *Id*.

12. *Id*.

point person and to coordinate the diligence process, and a diligence team with clear objectives and subject-matter expertise. The proper team is particularly important with respect to data privacy and security diligence, which may fall outside of the expertise of traditional M&A lawyers.

B. Considerations in Conducting Data Privacy and Security Due Diligence

1. Due Diligence on Data Privacy and Security Issues Should Not Run Afoul of Prohibitions on "Gun-Jumping"

Exchanging information prior to the consummation of a transaction is appropriate so the parties may properly structure the deal to ensure they are receiving the benefits of the bargain. Competition laws generally permit the disclosure or exchange of such information, including competitively sensitive information, as part of the due-diligence process. However, the disclosure or exchange of certain information—or using such information to integrate the acquisition prior to closing—can constitute "gun-jumping" in violation of civil or even criminal antitrust enforcement under, for example, Section 1 of the Sherman Act or Section 7A of the Clayton Act. In addition, the Antitrust Division of the Department of Justice has interpreted the Hart-Scot-Rodino (HSR) Act to prohibit an acquirer from exercising "substantial operational control" over an acquired company prior to the expiration of the HSR waiting period.[13] As a general matter, the disclosure or exchange of information relating to data security will generally be judged under the "rule of reason" as opposed to "per se" treatment under a naked

13. *See* Complaint for Equitable Relief and Civil Penalties at 15, United States v. Gemstar-TV Guide Int'l, Inc., No. 1:03 CV000198 (D.D.C. Feb. 6, 2003), ECF No. 1.

anticompetitive restraint.[14] Parties should, therefore, be cognizant that any exchange of information undertaken in conducting due diligence relating to data security issues is designed for that purpose and not unrelated purposes that might, for example, be used as evidence to support a claim of "gun-jumping."

2. Deal Considerations

While all acquisitions would benefit from some level of data privacy and security diligence, there is no one-size-fits-all approach, and the data privacy and security diligence will vary deal to deal. The focus, scope, and significance of the data privacy and security diligence review will depend on a number of factors, including:

- the transaction size and complexity;
- the transaction structure;
- the ongoing obligations of the parties;
- the type of location of any relevant sensitive information;
- cross-border considerations; and
- the industry.

These considerations will likely drive the scope of data privacy and security diligence and are initially analyzed by the buyer or party undertaking the analysis.

(a) Initial Steps

Data privacy and security should be considered in acquisitions for two primary reasons. First, as discussed in more detail in various other sections herein, the buyer should investigate the target's privacy and security practices to analyze the risk and adjust the deal value. Second, both parties have a duty to maintain confidentiality, privacy, and security during the

14. *See* United States v. U.S. Gypsum Co., 438 U.S. 422, 438 (1978).

transaction. This is especially critical during the diligence process, where sensitive information of both parties is accessed and shared.

In light of these privacy and security concerns, prior to starting the diligence process, the parties should execute a nondisclosure agreement (NDA) to establish the terms of data sharing and set forth the restrictions and protections for that information. The NDA should limit the scope of data access and use and describe any additional protections for particularly sensitive or regulated information, such as Personally Identifiable Information (PII), Protected Health Information (PHI), credit card information, or trade secrets.

Once an NDA is negotiated and executed, the buyer will have an opportunity to make specific requests regarding the information it would like to review during diligence. The seller will then attempt to complete the buyer's diligence checklist by providing relevant information and documents. Then, the target will attempt to fill out the checklist and provide the requested materials. Typically, this is done via a traditional or virtual data room (VDR), which can be created by one of the parties, an agent of one of the parties, or a third-party data-room provider. In setting up a VDR for a transaction, the transaction parties should consider the following:

- Who will be responsible for hosting the VDR?
- Who owns the data in the VDR?
- What security measures will apply to the VDR?
- Who is liable for a breach of the VDR?

VDRs can be hosted by the transaction parties (e.g., through a company-run Dropbox or File Transfer Protocol (FTP) site), an agent of one of the parties (e.g., an investment banker or broker), or a third-party VDR provider. If one of the parties is hosting the data room, the parties should make clear who owns the data

and the privacy and security protocols. Typically, each party will own the data it uploads, with access and use subject to the NDA. If a third party is hosting the data, the transaction parties should carefully review their engagement letter or service agreement with the third party and identify the allocation of risk and security protocols and compare these to the costs of the services.

(b) The Virtual Data Room

VDRs have emerged as a technology-based due-diligence tool used to facilitate access for purposes of disclosure and document sharing in M&A transactions. VDRs allow companies to maintain and share critical business information in an online environment, streamlining all stages of the document and communications process. In connection with such transactions, these internet-based document repositories capture, transmit, handle, and store confidential, proprietary, and sensitive information regarding their customers and clients of their customers.

Due to the increased reliance on VDR technology and the amount of sensitive data shared during typical M&A diligence, data security is a primary concern in preparing and using a VDR. Unauthorized access to a VDR could result in widespread, irreparable damage to any number of parties, as well as to the deal itself. Unauthorized access or disclosure of proprietary information caused by a compromised VDR can negatively impact the value of a business, its market share, investor return, and competitive advantage. This is especially true in the context of M&A diligence where data rooms often contain highly confidential information, such as pre-initial-public-offering due-diligence reviews, bankruptcies and restructurings, audits, proprietary intellectual property, employee or customer PII and PHI, and fundraising initiatives. The unauthorized access or disclosure of this type of information can have significant economic

consequences on all parties. Therefore, strong data protection and cyber security practices are essential.

In order to engage a VDR service provider and gain access to its platform, prospective customers enter into contractual arrangements. Companies and their advisors should thoroughly vet their VDR service providers to ensure the VDR is adequately protected throughout the diligence process. The amount of security required could vary depending on the deal considerations, but standard VDR security should address the following:

- strong username and password controls;
- industry-standard encryption options;
- deterrence features, such as watermarking;
- access control, such as view-only;
- lock-down procedures; and
- partitioning and the availability of additional security for highly sensitive information.

Many of these security functionalities within a VDR are referred to collectively as "Information Rights Management" (IRM) tools. Ensuring the VDR selected for a particular transaction has the necessary IRM capabilities should be a threshold inquiry.

Customers that enter into agreements with VDR service providers must be cognizant of the allocation of risk and damage limitations that apply to security-breach situations. VDR agreements often require the customer to bear sole responsibility for monitoring, preventing, and notifying the VDR service provider of unauthorized access.

(c) Beyond the Data Room

Although data privacy and security review is becoming more prevalent in M&A diligence, current diligence practices that attempt to incorporate data privacy and security issues are generally still subject to traditional diligence limitations,

including the lack of context regarding the data being shared in the VDR and often limited access to key personnel. This is further complicated by the significant inconsistencies in how companies deal with data privacy and security due to the lack of a "standard" in this space.

Because of this, and because of the importance of data privacy and security, buyers may request additional diligence beyond the data room. This is particularly prevalent in transactions with highly sensitive information or significant potential liabilities. In such transactions, the buyer may request that the target share the results of its most recent security audits, penetration tests, or other vulnerability assessments, or even undergo independent third-party assessments as part of the diligence process if such information is not available or up to date. The target's willingness to undergo additional assessments will likely depend on the cost of such assessments relative to the value of the transaction and the buyer's negotiating position. Where, for instance, a buyer is permitted to engage in an additional assessment, it must identify the right people within the target to query. Because critical people often leave before an acquisition or asset purchase is finalized, having direct access to these individuals before the transaction is beneficial, as this information will be much more difficult to obtain post-closing. Once the individuals are identified, each of the categories and types of data identified in Appendix A should be explored.

(d) Types of Data

In conducting due diligence, the buyer should obtain a thorough understanding of the types of data maintained by the target, and, in turn, which categories of data the parties intend

to include and exclude from the transaction.[15] This information will help potential buyers understand: (i) the laws applicable to the data; (ii) whether consent is needed to transfer the data (under data protection laws); (iii) the types of security required to protect the data; and (iv) how to integrate the target's digital assets into the buyer's final information technology (IT) infrastructure. The diligence will further allow the buyer to identify and evaluate data protection concerns (and documentation about the way in which they were dealt with) to determine how much of the existing infrastructure and practices can be drawn into the new organization. In addition, diligence on the data types may provide information on how the potential purchaser will be able to access data protected by passwords and data stores with limited access rights. These inquiries may incorporate questions regarding how any data migration will impact the business-continuity procedures of the buyer and may influence the ultimate deal.

(e) Where the Data Is Stored

The locations where the target keeps data, and why and how the data function is integrated within the target, may also influence the ultimate outcome and value of the deal. The potential buyer must be satisfied, for example, that the target has retained adequate records required by federal, state, and foreign law, as well as by the internal policies of the target. If data is located in countries with strict data protection laws, the target will have to consider the measures that must be taken to secure, process, and transfer that data in accordance with applicable laws. The

15. In conducting the above diligence, it is helpful to determine automatic-deletion periods, retention periods, and backup tape practices of the target. To the extent the target lacks an adequate retention policy, there may be excess data stored with the target that need not be transferred as part of the transaction to save costs of storage and future destruction of data.

location of data may also implicate employee monitoring of emails and other human resource (HR) functions, as well as customer consents.

Much of the knowledge regarding the location of the target's data likely resides in a corporate data map or with the target's corporate records manager. If there is no central policy or point of responsibility, another avenue of inquiry is into existing information governance projects.

The following information will help to identify the locations where the data is stored:

- A schedule of all in-house servers, Network Attached Storage document management systems, or data warehouses maintained by the target
- A schedule of all cloud computing services/collaboration services used by the target
- Whether each service is hosted internally or by a vendor other than the target
- A schedule listing all personal computers owned by the target. For portable computers, determine whether encryption is applied at the drive level.
- Whether the target provides or permits the use of portable hard drives (USB drives) for business purposes, and the controls applied for approved uses
- Whether information of the target resides only on target-owned devices, or may also reside on employee-owned devices (e.g., smartphones, tablets)
- Whether employee access to "self-help" cloud computing services (e.g., Gmail, Google Drive, Dropbox, Evernote) is allowed or prohibited

For data that is being hosted by outside vendors, the buyer should obtain copies of service agreements, including data security and privacy obligations of the vendor. The provisions in these agreements on which to focus include the following:

- *Security Provisions:* Assess whether the agreements contain adequate language on how a vendor is required to secure the data of the target.
- *Audit Rights:* Evaluate whether the target has the right to audit the vendor to ensure the security of the target's data.
- *Data-Breach Language:* Evaluate whether the agreements have language addressing:
    - the vendor's notification responsibilities in the event of a data breach;
    - whether the vendor is required to indemnify the target for a data breach;
    - whether the vendor is required to cooperate with the target in the event of a breach; and
    - damages-limitation clauses in the event of a data breach.
- *Data Protection Language:* To the extent a vendor is hosting data that is governed by foreign data protection laws, the agreements should contain detailed language regarding which laws apply and explain that the vendor is acting as a data processor.
- *Ownership and Access:* Confirm that the target has maintained ownership and access rights to the data stored on the outside vendor's hosted environment.

(f) Review of Privacy Policies and Related Compliance

The due diligence associated with the deal should incorporate a consideration of data privacy issues. For those deals involving multinational organizations (which might simply mean the collection of data from multiple countries), the issue of privacy rights violations is beginning to take on the same level of concern that traditional antitrust reviews have had.[16] This privacy policy review step should incorporate privacy policies provided to employees and other personnel. The review should consider the availability and composition of consent forms relating to collection, storage, and use of data, whether such forms are updated over time, and whether they are consistent with current use. The review should examine consumer-facing privacy policies, evaluate whether privacy policies comply with current Federal Trade Commission (FTC) expectations,[17] and determine whether privacy policies are followed internally at the target.

This review should also consider those privacy policies provided to the target's customers, its suppliers, and the general public—especially with language permitting acquisitions in mind, as the permissions incorporated into those policies may determine exactly how the buyer may use otherwise-private data post-deal.[18] These issues may be addressed by reviewing

16. Kakoli Bandyopadhyay et al., *A Framework for Integrated Risk Management in Information Technology*, 37 MGMT. DECISION 437 (1999).

17. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

18. *See* Letter from Fed. Trade Comm'n to Hon. Shelley C. Chapman regarding *ConnectEdu, Inc.*, No. 14-11238 (Bankr. S.D.N.Y.) (May 22, 2014), https://www.ftc.gov/system/files/documents/public_statements/311501/140523connecteducommltr.pdf.

both the existing data collected, and also by reviewing and cataloging changes in the target's privacy policies over time. Not all data will necessarily have the same permissions attached to it. This review should always incorporate compliance with state laws,[19] as well as international law when warranted.[20]

(g) Information Governance Policies and Record Retention Schedules

Despite the importance of information governance policies and record retention schedules, they are not often considered in the context of deal due diligence. This is not surprising. Even IT infrastructure and post-deal integration is sometimes an afterthought.[21] Still, given the rapid growth in data and its effect on deal considerations,[22] a request for and review of available data retention policies and record retention schedules should be at the forefront of the due-diligence process. The practitioner should confirm that existing policies address each of the data locations identified during the deal due-diligence process.

Next, the buyer should square the policy and schedule information with considerations regarding privacy policies and related data, confirming the policy identifies data types as well as levels of confidentiality (e.g., sensitive consumer PII, classified, confidential, and public). This confirmation process may also determine whether the policies and schedules are reasonable

---

19. The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, 17 SEDONA CONF. J. 1 (2016).

20. Donald C. Dowling Jr., *How to Ensure Employment Problems Don't Torpedo Global Mergers and Acquisitions*, 13 DEPAUL BUS. L.J. 159 (2000).

21. Monideepa Tarafdar & Sufian Qrunfleh, *Examining Tactical Information Technology—Business Alignment*, 50 J. OF COMP. INFO. SYS. 107 (2010).

22. Paul P. Tallon, *Corporate Governance of Big Data: Perspectives on Value, Risk, and Cost*, 46 COMPUTER 32 (2013).

considering the level of confidentiality and business needs for access to the information.

Legal hold practice stands as the exception to the proverbial rule, where certain portions of the information governance policy and record retention schedule may need to be suspended based on retention periods and automatic data transfers or deletions. The buyer should determine whether appropriate safeguards are in place to suspend schedules during litigation holds. This may include practices specific to the deal itself, where information associated with the deal might relate to subsequent deal litigation.[23] A good start for this type of analysis may be a review of existing legal hold practices, policies, and other related information, which would then be read in conjunction with the policies and schedule.

(h) Determine Applicable Automatic-Deletion Periods

A number of organizations—as well as individuals acting on their own—have automatic-deletion policies. For example, it is not uncommon to have email management policies that delete email after certain periods of time, or when email is moved to other locations within (or outside) the email program. As noted in prior guidance, "an automatic deletion policy is coupled with options so that the user can move email of significance to an appropriate alternative storage location."[24] Advisors to the acquisition process, especially those involved in post-deal integration activities, should determine whether any of these rules-based systems would apply in the integrated environment and whether any legal holds apply that would require the

23. John C. Montana, *Retention of Merger and Acquisition Records and Information*, 34 INFO. MGMT. J. 54 (Apr. 2000).

24. The Sedona Conference, *Commentary on Email Management: Guidelines for the Selection of Retention Policy*, 8 SEDONA CONF. J. 239, 241 (2007).

suspension of any automatic-deletion practices.[25] This issue may also determine whether any of the automatically deleted data should be collected pre-integration while still available, perhaps in connection with a prior or prospective legal hold.

(i) Determine Backup Tape Practices

Backup tape practices in support of organizational information technology practices may be determined by reference to International Organization for Standardization (ISO) standards. In addition, certain compliance groups may retain backup tapes and related materials in accordance with regulatory standards—this type of transition (or lack thereof) has caused issues for merging organizations.[26] Finally, there may be exceptions to normal practices associated with backup tapes pursuant to existing legal holds,[27] where information technology professionals may or may not be aware of what the legal department has sequestered in accordance with those holds.[28]

(j) Review Warehousing (Including Third-Party) Practices

While warehousing issues are uncommon in current M&A due-diligence approaches,[29] they remain an important part of

25. EEOC v. JP Morgan Chase Bank, N.A., No. 2:09-cv-864, 295 F.R.D. 166 (S.D. Ohio 2013).

26. Sherer, *supra* note 9 (citing Order Instituting Administrative and Cease-and-Desist Proceedings at 2, UBS Sec. LLC, Exchange Act Release No. 52022 (July 13, 2005) (Admin. Proc. File No. 3-11980)).

27. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1 (2018).

28. *See* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

29. James A. Sherer et al., *Merger and Acquisition Due Diligence Part II—The Devil in the Details*, 22 RICH. J.L. & TECH. 4 (2016).

post-deal integration activities, especially where such activities may include "warehouses of poorly organized boxes" instead of clean, well-managed, and ordered records.[30] A review of such practices should incorporate both a policy review as well as an interview step with the target subject-matter expert knowledgeable about or responsible for such activity.

3. Existence of and Implementation of Data-Classification Policies and Related Security Measures

In addition to considering the location of information, the type of information (including whether it is comprised of or contains PII or PHI), and the manner in which the information is stored or deleted, the buyer should also consider a review of data-classification policies. This review would confirm that existing policies or schedules classify data according to its level of sensitivity. The buyer should also consider the impact to the target should that data be disclosed, altered, or destroyed without authorization according to the data's characterization (e.g., private, sensitive, internal, public). For government-contractor data or related reviews, this evaluation might also consider whether policies comply with FIPS PUB 199.[31] This evaluation would begin by obtaining and reviewing baseline security controls for each classification. The review would then confirm whether baseline security controls are appropriate for safeguarding that data.

Depending on how highly sensitive data is categorized and treated, there may be sensitive data-specific repositories within the target as well. Consideration of this point should

30. Montana, *supra* note 23.

31. U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., COMPUT. SEC. DIV., FIPS PUB 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS (Feb. 2004), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

incorporate further investigation of the policies detailing how data classified as highly sensitive is handled, as well as reviewing employee training materials that implement such policies.

For data classified as "sensitive," the buyer should determine whether the target has a policy to encrypt the data in transit and at rest. Finally, the buyer should consider whether the target has implemented technical controls to enforce that policy. This review will determine how the buyer may access data in company/security access controls post-deal, perhaps by determining the criteria used for granting access to each service or data repository (e.g., whether criteria permits access only to employees having a business need for that access).

In addition to determining what data should be classified as sensitive, the buyer should determine whether the information is being protected. This requires a review of affirmative security systems and requirements associated with the data, which begins with a determination of what systems are in place and how they are documented. IT and general security are often mature functions within most organizations, and there should be a number of straightforward policies available for due-diligence review, including wireless internet service providers. In addition to those policies and interviews with responsible parties, we suggest that the buyer make plans for affirmative post-deal physical-security activities, as these might slip through the cracks during integration. These physical security activities include: (i) engaging a third-party security consultant to audit for vulnerabilities; (ii) establishing a monitoring program; (iii) identifying physical security procedures for employee, contractor, and third-party workers; and (iv) evaluating third-party requirements for physical security.

4. Business Critical Functions

There is data that is classified, and data that is critical to the ongoing operations of the target organization. While the two are not mutually exclusive, organizations often build out a separate practice for bringing the organization back "online" given a disaster or other failure—in whole or in part—of the enterprise's operations.[32] The due diligence might begin with an evaluation of the target's disaster-recovery and business-continuity plans. But instead of stopping at the four corners of the plans, the buyer should also determine: (i) whether it will substitute its own policies or plan for assets pre- or post-integration; (ii) whether the plans are all-or-nothing propositions, such that the buyer might implement a disaster-recovery plan and identify basic provisions of that plan; (iii) how such implementation might work; and (iv) what, if any, are the third-party requirements associated with such disaster-recovery and business-continuity plans.

The buyer might also undertake a business impact analysis of business-critical systems (e.g., order entry, manufacturing, shipping, receiving), determining which processes, systems, and data are most critical to the continued business operations of the target. This should lead to the next steps: understanding what additional systems are dependent on business-critical systems, and assessing the consequences of losing such systems. The buyer should also obtain and evaluate backup and disaster-recovery plans for business-critical systems, perhaps in conjunction with an evaluation of the backup tape system. Finally, the buyer should evaluate whether resources and priorities allocated to the recovery of business systems are commensurate with the criticality of the systems.

32. Balachandra Reddy Kandukuri et al., *Cloud Security Issues*, 2009 IEEE INT'L CONFERENCE ON SERVS. COMPUTING.

5. Due Diligence Beyond the Data Room

In addition to the reviews of policies and technical specifications of the target's information systems and data flows, separate interviews with target employees regarding how data is really collected, stored, and used are likely to be helpful. Unfortunately, this information may walk out the proverbial door during the pendency of the deal or after its conclusion.[33] When available, these interviews should be carried out with representatives of the target's IT, HR, C-suite, and "other" functions. For IT, discussions should consider current employee access as well as third-party employee access, and how those might change during the process where the target's systems are integrated into the buyer's policy and IT environment. Likewise, HR representative interviews might further examine both the documented policies and procedures associated with information capture, storage, use, and disposal as well as the realistic practices within the organizations.

While the C-suite executives may not be well-positioned to talk about the use of information at every level of the organization, the information in their possession may be paramount for continuing operations post-integration. The buyer should focus on both the preservation of that information as well as any data generated in the meantime. Finally, depending on the operation of the target, the buyer should examine who else might be part of the target's information lifecycle. These participants may include: (i) providers of sourcing or supplier activities (and their agreed-upon compliance metrics); (ii) other third parties or cloud providers that host information; (iii) customer data and records of interactions (e.g., portals); and (iv) social media and related marketing, advertising, and sales platforms.

33. Sherer, *supra* note 9.

C. *Adapting the Due-Diligence Process to the Changing Terms of the Deal or Information Being Provided*

During the due-diligence phase, the parties may need to supplement or alter their due-diligence requests or the proposed representations and warranties that form the backbone of the transaction. Frequently, the transaction is on hold during the due-diligence process because the information disclosed through the due-diligence process could have significant impacts on the proposed transaction. By this point, a term sheet, letter of intent, or similar document may be in place (along with the NDA), and draft transaction documents may be circulated. But details are typically not finalized until after diligence takes place. During the due-diligence phase, one or both parties to the proposed transaction could obtain information that affects the negotiation, deal structure, and the draft documents, or that could potentially derail the deal. Early due-diligence responses could also lead to follow-up due-diligence requests as the parties try to refine their understanding of one another and the proposed transaction.

Follow-up due-diligence requests may seek additional information or additional support for prior responses. The data and documents shared during due diligence can identify undisclosed assets or liabilities, title issues, incompatibilities or inefficiencies, cultural or "fit" issues, tax considerations, additional costs, compliance issues, or other critical, nonpublic information. This new information could impact the value of the deal, the representations and warranties of each party, the asset-disclosure schedules, or post-closing integration and migration. Because of this, the diligence process often leads to new rounds of negotiation and revised transaction documents. For example, when Verizon learned that Yahoo, its acquisition target, had suffered two large-scale data breaches prior to the acquisition closing, Verizon immediately halted the closing and sought

additional information (in addition to a substantial reduction in the purchase price).

If the parties are unable to resolve issues identified in the due-diligence process, the transaction could be postponed or killed. These post-diligence considerations are particularly important in the privacy and security context where assets are sensitive, compliance can be complicated and burdensome, and latent incidents may go undiscovered for years in the normal course of business. In this context, the information and documents exchanged in the due-diligence process may require the parties to update schedules of included or excluded assets and liabilities (including data, data-streams, licenses and permissions, and hardware), revise or extend data privacy and security representations and warranties, or adjust plans for post-deal information technology and information security migration and integration.

D. Stage Two Summary

During the due-diligence phase of the deal, the parties should:

- identify a deal team "quarterback" with data privacy and security expertise;
- assess the type of sensitive information involved, the location of sensitive information, the target's current and historic data security and privacy practices, known vulnerabilities and breaches, and the target's relationship with vendors;
- execute the necessary NDAs to establish the terms of data sharing and set forth the restrictions and protections for that information;
- determine responsibility for creation and maintenance of a VDR to share information

requested in the due-diligence phase and determine responsibility for the privacy and security controls over the VDR itself;

- consider whether any due diligence needs to be conducted outside of the VDR and perform all necessary analyses;
- obtain a thorough understanding of the types of data utilized by the seller and the specific data that is being included or excluded from the transaction;
- interview any necessary personnel or third-party vendors regarding how the relevant data is collected, stored, or used by the seller;
- determine where the relevant data is stored by the seller;
- review the target company's privacy policies and notices, the target company's compliance with those policies and notices, and the target company's compliance with international, federal, state, and local laws and regulations;
- review available data retention policies, document retention schedules, automatic-deletion schedules, backup tape processes, and warehousing practices;
- review data-classification policies and related security measures;
- assess the target company's disaster-recovery and business-continuity plans and determine whether and to what extent the target company or the purchaser's plan will govern post-closing; and
- determine whether any existing due-diligence requests or representations and warranties need to be supplemented, modified, or

terminated based on the information acquired during the due-diligence phase.

IV. STAGE THREE: CLOSING AND POST-CLOSING CONSIDERATIONS

Post-deal integration of information technology and information security systems simultaneously presents great challenges and great opportunities. Historically, records and information management was an afterthought in an acquisition, where the speed to close the deal took priority over the practical considerations of running the acquired business. In most transactions, the buyer simply took possession *en masse* of the seller's electronic and hard-copy records and dealt with them. Sometimes the buyer would merge the seller's records with its own records, other times the buyer would maintain separate systems running in parallel, and still other times it would place the records in offsite storage or equivalent "just in case," perhaps discarding some categories of records that were deemed not to have ongoing value.

Today, the "take it all and sort it out later" approach often has significant downsides. In addition to the hard and soft costs associated with storing enterprise data (which some estimates have placed at $5,000 per terabyte or more), over-retention of data can needlessly create serious legal, regulatory, and business risks. Today buyers are finding that when it comes to data privacy, the old saying that "possession is nine-tenths of the law" could not be further from the truth, and that if care is not taken to ascertain what rights the buyer has to use and transfer personal information collected over time from customers, clients, and others, some or all of the buyer's plan to extract value from that information could be thwarted.[34] All modern companies possess large stores of electronic information. As a result,

34. Letter from Fed. Trade Comm'n, Bureau of Consumer Prot., to WhatsApp and Facebook (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

any transaction involves significant information assets. Those assets should be an integral part of the diligence process and receive prompt attention upon closing.

A. Mechanisms for Allocating Information-Related Risks

In many ways, the risks associated with data privacy and security are no different than the myriad other contingencies that are addressed by buyers and sellers during due diligence, negotiation, and post-closing dealings and, accordingly, often can be addressed using familiar tools. A full discussion of such tools, and when and how they can best be used to apportion information-related risks between buyers and sellers, is beyond the scope of this *Commentary*; however, two common examples warrant brief mention.

1. Purchase-Price Adjustments

Purchase-price adjustments are common in private-company acquisitions. Generally, for example, if an acquisition has a closing date separate from the date of the signing of the purchase agreement, a working-capital adjustment often is part of the transaction documents. This adjustment is in place to capture any change in the target's working capital between the date the purchase agreement is signed and the final closing of the transaction. While working-capital adjustments are ubiquitous in non-simultaneous sign-and-close transactions based on some valuation for the seller's working capital post-closing, purchase-price adjustments may be included to address any change in the value of the underlying assets between signing and closing. A purchase-price adjustment may be triggered by a new potential liability, such as a data breach that occurs between signing and closing, or upon request by the buyer in response to changes in valuation uncovered during due diligence. A prominent example of this is, of course, the Verizon/Yahoo acquisition discussed earlier.

Although most purchase-price adjustments are made in response to specific items impacting the financial statements of the company like working capital or EBITDA (earnings before interest, taxes, depreciation, and amortization), it may be appropriate to adjust the purchase price based on the occurrence of certain events during the gap period between signing and closing or in response to diligence discoveries. Events related to data privacy and security that may depress the value of the target company could include: (i) a data breach or other security incident requiring notification to data subjects or regulatory response; (ii) contractual or other limitations on the seller's ability to transfer valuable data to the buyer; (iii) inability on the buyer's part to use such data in ways that were anticipated when it made the initial offer of purchase; or (iv) identification during due diligence (or even post-closing, if the transaction documents permit) of data that is not collected, stored, used, or disclosed in a manner that is consistent with the company's policies or applicable law.

2. Indemnification

Sometimes, a purchase-price adjustment is not a feasible way to control for an issue that comes up during negotiation of the transaction. This may be particularly true where the underlying business will not be impacted by the issue. But there will likely be a tangible cost to addressing it, whether in legal fees, remediation measures, damage to brand or reputation, or regulatory penalties. Alternatively, if the issue is speculative and may never accrue any costs, but the buyer wants coverage on the chance that any such costs do accrue, a purchase-price adjustment may be hard to negotiate. In this instance, a special indemnity may provide the comfort the buyer requires to close the transaction without reducing the purchase price. A special indemnity can be structured so it is not subject to any basket or cap in place for the general indemnity. This will allow the buyer

to receive indemnity from the first dollar on any post-closing costs that are incurred by the company for data-related issues that may have accrued prior to closing. If the potential issue never materializes or otherwise does not result in any harm to the buyer, the special indemnity impacts neither party. But the buyer still maintains coverage for the length of the term of the special indemnity.

B. Post-Closing Operational Issues

It is important for the buyer to consider post-closing operational issues early in the transaction and consider them carefully during the drafting of the transaction documents. Issues like transferability of data, evaluation of IT infrastructure and data mapping, separation and integration of data, and harmonization of privacy and security policies should be considered as the transaction is proceeding, and may even be important for the buyer to understand when deciding whether to acquire the seller's business operations or assets in the first instance. It is important for the buyer to make an up-front determination regarding whether the data held by the seller can be used in the way the buyer contemplates and the extent to which the systems being purchased will create synergies or headaches for the buyer. In addition, as soon as practical after the closing of the transaction, the buyer should undertake to determine whether the data transferred as part of the transaction is consistent with the agreement, including its representations and warranties.

1. Identification and Confirmation of Data Transferred

While many transactional documents typically have long schedules of assets transferred, it is atypical for such documents to include a listing of the data, much less data maps identifying the data, its physical location, the hardware associated with the data, and other information necessary to access or query such data, including passwords, encryption keys, instruction

manuals, and field listings. Often, some or all of the IT personnel necessary to ascertain that information are no longer available or accessible post-transaction. Similarly, data may often be transferred but without the necessary hardware or software to access and manipulate the data.

Thus, as a threshold matter, the buyer will want to understand exactly what type of data it now owns as a result of the acquisition and what data, if any, is merely custodial or transient to its systems. This process can be a formal undertaking done through an inventory of the data or can be as informal as a perusal of a file share, depending on factors such as the volume, value, and risk associated with the information. Inventorying the data will simplify the process of understanding what data the buyer has, how it can be transferred or used, and whether it can be easily combined with the buyer's existing data. This process also should involve reviewing and, to the extent necessary, merging the buyer's and seller's respective record retention schedules, as well as identifying and taking appropriate steps to protect data coming from the seller that is subject to a litigation hold.[35]

2. Segregation of Data

The commingling of data once done is difficult to undo. Accordingly, prudence—as well as legal, technical, and practical reasons—dictates that a buyer should not immediately merge acquired data into its operations. Examples of data that require caution before merging are: (i) internal individual data (such as employee data); (ii) external individual data (such as customer or consumer data); (iii) data sets used specifically in performing a service (such as mapping data); (iv) data held by the company

35. *See* ILWU-PMA Welfare Plan Bd. of Trs. v. Conn. Gen. Life Ins. Co., No. C 15-02965 WHA, 2017 WL 345988 (N.D. Cal. Jan. 24, 2017) (sanctioning company for loss of data transferred during sale of business).

as custodian for a third party (such as data hosted by a service provider for corporate clients); and (v) transient data (such as data being processed or transmitted through the company's servers but to which the company has no ownership or other rights). The buyer should carefully consider and develop a strategy for the transfer, migration, use, and disposition of the acquired data.

3. Right to Use and Transfer Data

Purchasing a company does not automatically allow the buyer to use or transfer to itself or its affiliates (in the event of a stock sale or merger) the data owned by the target company. Transfer of any data outside the confines of the corporate entity that owns it, as well as use of the data by any affiliate or third party, may be subject to pre-existing obligations, whether contractually or through stated policies, such as a publicly available privacy policy at the point of collection. Whether already undertaken as part of the due-diligence process, it is important to review any pertinent existing privacy policies (including historically applicable policies) prior to the transfer or use of any consumer data obtained through an acquisition. If these policies limit the seller's ability to transfer the data, such restrictions likely will continue to apply post-closing, and the data may be required to remain within the acquired company or risk regulatory action. In addition, if the uses to which the buyer plans to put the information post-closing differ materially from those permitted under the seller's policies in effect at the time of collection, the buyer may have to obtain consent from the data subjects for such new uses.

4. Contractual Restrictions

Restrictions on the data may arise from promises made between the company and its users through the publication of a privacy policy. But restrictions may also exist through direct

contract between the company and its clients, customers, or vendors. Pay particular attention to any contractual arrangements that may limit the buyer's use of data held by the company post-closing, especially if the company is a custodian of data owned by others. Before putting any data collected or stored by an acquisition target to use, the buyer should review any agreements that may govern the use, retention, and disclosure of the data to ensure that no data is being treated in a way that conflicts with the company's contractual obligations. If there are any use restrictions inherent in such agreements that are not part of the existing data-use policy of the post-acquisition company, the buyer may need to revise any policies to address such additional restrictions. If the data is required to be used or stored in a manner inconsistent with prior uses based on fundamental business needs post-closing, the buyer may need to renegotiate certain agreements to provide for these new uses. As further discussed below, all acquired data should remain segregated from the buyer's data until the buyer has had a chance to: (i) understand the scope of the data in the company's systems; (ii) review the pertinent use and transfer policies for the data; (iii) cull any low-value data; and (iv) structure a plan to handle the data on a going-forward basis.

5. Statutory and Regulatory Restrictions

Beyond contractual provisions, many types of data are subject to statutory and regulatory restrictions to include data privacy, state security, and export control. The fact that data was acquired in a transaction does not give the acquiring party the unfettered right to either access or use the data. For example, in the European Union, personal and private data of the employee is just that—property of the employee. It is a violation of the employee's human rights to process that data, for example, without notice and permission. The recognition and application of these rights are being expanded under, for example, the

General Data Protection Regulation (GDPR). Accordingly, the buyer should undertake careful consideration of these and other statutory and regulatory rights ***before*** it accesses, transfers, or uses the acquired data. Be careful if the buyer intends to physically transfer the data from one country (for example, where the seller or data resides) to another country (for example, where the buyer or its facilities reside).

6. Data Separation

Not all transactions involve a transfer of all data from the seller to the buyer. Divestitures in particular present thorny issues that generally are not present where the entirety of a business is changing hands. Because a divestiture ultimately is a sale by a parent of some portion of its assets and operations (e.g., a subsidiary) to a third party, the data that is transferred must be viewed through that same lens—that is, the parent is selling the data to a third party.

From the parent's standpoint, if it neglects to take reasonable measures to protect data that is not part of the subsidiary's operations and, therefore, should not be transferred as part of the divestiture, it risks running afoul of myriad data protection laws and regulations, even if the data remains entirely contained within the subsidiary and is not breached or transferred to other areas of the buyer's enterprise. And if the subsidiary experiences a breach that results in the parent's data being exfiltrated, or potentially even if the subsidiary merely transfers the data to other areas of the buyer's business, then cue the usual parade of horribles (e.g., civil litigation, regulatory enforcement). A similar analysis applies in the context of privilege waiver. If the parent fails to take appropriate measures to prevent privileged information from being transferred to the buyer as part of the divestiture, then it could be found in subsequent litigation to have waived privilege by transferring the information to a third party without taking reasonable steps to protect it.

On the subsidiary/buyer side, similar issues and risks exist. By failing to take reasonable steps to excise data that isn't part of the subsidiary's operations, the subsidiary and buyer are on the receiving end of a data transfer that potentially violates data protection laws. Again, this can be problematic regardless of a further transfer or data breach. A class of consumers, for example, might argue the transfer of data that was not properly part of the subsidiary itself was a breach because it was an unauthorized transfer. In the event of an external breach, this too can trigger a parade of horribles. Another issue for the subsidiary/buyer is that if it takes or receives protected data, it also assumes all of the legal and compliance obligations that attach to that data (e.g., obligations under some regimes to destroy data after expiration of purpose, and requirements to maintain certain types of information in secure environments).

A well-designed and executed framework for data separation is important because the parties need to understand the security infrastructure differences between the organizations and evaluate not only where data is located currently and what security measures are in place to protect different tiers of information, but also how those measures differ between the organizations and why. There may be infrastructure challenges that the parties need to fully understand and map out before data is migrated from one system to another. If not done pre-closing, a post-closing review of the full universe of relevant systems to be integrated (or divested if there is a spin-out or other split in systems) can assist the parties to understand the scope and landscape being considered for integration, migration, or separation. In addition, a review can help determine where policies can be harmonized and can help the parties understand what data should be integrated and what data should remain segregated.

7. Deletion of Data

Once the data has been inventoried and its existing limitations understood, the buyer can then determine whether any of the data is low-value data that should be deleted rather than combined with buyer's existing data. The Compliance, Governance and Oversight Counsel estimates that approximately 70 percent of average enterprise data is redundant, outdated, or trivial (ROT), and of little or no value to the business that stores it.[36] If the data has no legal or regulatory reason for its retention and is otherwise redundant, outdated, or trivial to the business of the purchaser, the purchaser should not pay to store it and risk its compromise through a security breach. Consideration should be given to purging data that can be identified as ROT before the integration process begins and before such data is integrated into the information systems of the buyer. Data deletion, however, is not without considerable risk unless undertaken in a defensible manner that takes into consideration legal, regulatory, and business requirements to maintain the data.

C. Best Practices for Data Integration

It is also important for the buyer to consider data integration strategies and best practices to ensure the business operates smoothly after the deal closes. If possible, the buyer should anticipate potential hurdles and roadblocks to integration and address these issues in the early stages of the transaction. The following are some best practices to consider when planning for integration after the transaction closes.

---

36. Deidre Paknad, *Defensible Disposal: You Can't Keep All Your Data Forever*, FORBES (Jul. 17, 2012, 10:40 P.M.), https://www.forbes.com/sites/ciocentral/2012/07/17/defensible-disposal-you-cant-keep-all-your-data-forever/#362f67bd6bb3.

1. Summarizing Limitations and Permissions

It is unlikely the legal or compliance officers who review the permissions around the data will be the same persons completing the technical process to integrate the data on the systems or using the data once it's been integrated. Once the review is completed, a memorandum should be prepared that summarizes the inventory of data and any limitations or restrictions to use, combine, and disclose the data acquired at closing. The memorandum will not only assist with planning and executing the data integration, but it also can serve as a "use guide" going forward when questions arise whether certain data can be used in certain business operations. Information that the use guide contains can be relevant to operations, marketing, IT, and many other areas of the business.

2. Leveraging Institutional Knowledge

As part of the integration process, the buyer may want to involve the seller's officers and personnel (as well as vendors, SaaS providers, and cloud providers) originally associated with the information to the extent possible. If the acquisition is structured as a stock sale, much of the institutional knowledge will likely now be captured by employees of the buyer. If the sale is structured as an asset sale, or in the case where certain knowledge resides in the chain above the target company, a transition-services agreement may be in place to assist with the transfer and integration of data. The buyer in that instance has maximum leverage in negotiating a transition-services agreement pre-closing. The buyer personnel should be informed of the transition assistance being provided and given an opportunity to capture as much institutional knowledge as possible from outgoing knowledge-holders.

If there will be redundancy in job duties and not all personnel will be transitioning to the business post-closing, those

employees taking over the duties of the departing ones should meet with their counterparts to determine the current practices in place regarding operations and data handling. They could then prepare written memoranda outlining the existing practices to smooth the transition. If emotions are raw or the systems to be merged are complex, it may make sense to engage a third party to consult on the integration and help streamline the combination of business processes.

3. Integration Meetings and Training

As part of the integration process, IT personnel and stakeholders for the various data types should meet so that all parties understand: (i) what data might be changing or is being added; (ii) who is responsible for the oversight and use of newly acquired data; (iii) how the data fits into the existing business operations; and (iv) whether any special procedures need to be adopted to handle newly acquired data. Employees who are expected to take on new responsibilities in managing data or privacy matters surrounding data need to be aware of these obligations and properly trained on the handling of information and the timeframes for compliance associated with any responsibilities.

4. Updating, Adapting, or Revising Policies and Procedures

It is a mistake to assume that data acquired as part of a transaction will fit neatly within the four corners of the buyer's policies and practices to include: (i) data privacy; (ii) data security; (iii) information governance; (iv) confidential information handling; and (v) information technology. Pay careful attention to whether and how such policies and practices require revision, adjustment, or adoption to fit the needs of the information that is to be acquired. This consideration is especially true when acquiring a new line of business (e.g., products, markets,

customers) that is not second nature to the buyer. Give particular consideration from a data security perspective to the acquisition of not only data, but also hardware associated with that data, or to providers or vendors with which the buyer has no prior business dealings.

5. Developing a Data-Transition Plan

Transitioning data from one entity to another may not be as simple as copying the data to a new location. Certain data may require physical safeguards to be properly maintained, applications that require additional licenses for full compliance, or additional equipment to be installed. The data-transition process should be reviewed in the aggregate with existing information, software, and systems to determine what overall schema will work best for the ongoing business. A sizeable acquisition of data may present an opportunity for the buyer to undertake a defensible deletion initiative, do a fresh security assessment, or otherwise find efficiencies and prospective compliance opportunities with respect to how it handles its data. If the target company processes, owns, or is custodian for a large data cache, then it may make sense to bundle the transition with other actions that may improve the buyer's compliance and cause long-run cost savings that can even recoup the entire amount spent on the integration.

6. Knowing When Not to Integrate

Integration is not the only option when it comes to handling post-closing data issues. As part of the due diligence, the buyer should closely examine the data in question, the universe of policies in place with both entities, and the reasons for and against integration. To the extent that the transaction is intended to combine two separate businesses into one business (to achieve operational efficiencies with economies of scale, to expand product offerings to existing customers, or even to roll

customers onto a new service), the ability to transfer data between organizations and to consolidate systems and policies typically will be desirable for the buyer.

There are situations, however, where it may make sense to forego integration altogether. For example, the seller is to operate independently to develop its own products and maintain its own customer base. Or the buyer purchased the seller with an exit strategy in mind, such as a portfolio company that may be sold after only a few years. In all scenarios, the buyer should remain aware of the potential pitfalls of transferring data from one business to another. It should avoid any transfers that might contravene the existing policies of the seller, are otherwise prohibited by the seller's public privacy disclosures, or violate existing agreements the seller has with third parties.

7. Recognizing Opportunities for Improvement and Advancement

As mentioned, an acquisition presents opportunities for operational improvements and advances. In any significant deal, substantial resources are allocated for due diligence, professional services, and post-deal integration. Business functions across the enterprise are focused on the many streams of work required to integrate successfully the new operations into existing ones. Critical human resources are still employed or otherwise available. And perhaps most importantly, as noted above, the seller's data is still separate from the buyer's data; it has not yet been integrated into the buyer's information systems. As a result, it can be assessed, analyzed, and acted upon without first needing to be identified and filtered from a larger set where it is commingled with the buyer's existing data. In short, many of the dynamics inherent in the acquisition process create ripe conditions for tackling many of the challenges inherent in that same process. Initiatives that might otherwise struggle in competition for funding, staffing, and other resources often can achieve

liftoff in their own right or by "piggybacking" on other related initiatives.

This pre-integration period of time provides an extra opportunity to not only review, analyze, and consolidate the data between the entities, but also to potentially find a structural solution superior to the one currently used by either entity. A buyer already investing in the integration process can take this opportunity to revise further its internal practices to a level that may bring it future cost savings in the form of enhanced economies of scale, reduced risk of security incidents, and streamlined systems that are less costly to maintain. The very real cost savings on a going-forward basis may justify the expenditure post-merger to reinvent the data management and security infrastructure of the transaction parties.

D. Stage Three Summary

The buyer should give consideration to the following issues that may arise during the closing or post-closing time period and, if needed, implement the appropriate measures:

- Whether the transaction should include a mechanism for allocating information-based risks, such as a purchase-price adjustment or indemnity provision
- A method for the identification and confirmation of the data acquired
- How the buyer intends to use and transfer the data, and any limitations that may exist (whether contractual, regulatory, statutory, or by virtue of the seller's existing privacy policies) on the buyer's ability to acquire, transfer, or use the subject data
- Whether the data being acquired is necessary to the buyer's operations, and how the buyer

will integrate the data into its operations on a going-forward basis

- Whether and to what extent data should remain segregated during the deal process and post-closing
- Under what circumstances it is necessary or appropriate to delete data that does not need to be transferred
- Creation of a memorandum summarizing the data acquired and any limitations or restrictions on its use, combination, and disclosure
- Development of a mechanism for capturing institutional knowledge and a plan for data integration, including training of relevant personnel
- Undertaking a holistic review of the data-transition process to determine how data will be integrated with existing information, software, and systems to determine what overall schema will work best for the purchaser's business going forward

APPENDIX A:
DIFFERENT CATEGORIES AND TYPES OF DATA IMPLICATED IN THE DEAL ANALYSIS

GENERAL CATEGORIES OF DATA	
CATEGORY	**DESCRIPTION**
Employee Data	Employee data includes Personally Identifiable Information (PII) of employees, such as names, addresses, and social security numbers. It includes banking and payroll information, such as salary data. This data can also include background check information and other sensitive information such as employee reviews, performance metrics, and disciplinary actions. Employee data is often particularly sensitive and thus triggers a range of regulatory requirements, including requirements relating specifically to background checks.
Customer Data	Customer data includes PII of customers, such as names and email addresses. It may also include customer preferences, such as purchase history or internet browsing habits, and customer account and billing information. Customer data is often the most valuable digital asset in an M&A transaction, but the uses to which the buyer can put acquired customer data can be impacted substantially by the acquisition target's privacy statements and privacy policies.

CATEGORY	DESCRIPTION
Intellectual Property (IP)	The IP that companies maintain will vary greatly in quantity and quality, and therefore IP is an example of how data classification is simple on the surface yet not so—it requires further stratification. Identifying all IP is not the same as classifying all IP, because different types of IP are afforded different legal protection and require different obligations of the holder of the asset. For example, the validity of a trade secret requires its holder to employ efforts that are reasonable under the circumstances to maintain its secrecy. Yet trade secrets are not the only type of IP to gain value as a result of secrecy. Thus, classification frameworks should consider other forms of IP, such as know-how and database contents.
Operational Data	Operational data may include the know-how referenced above. It may also include accounting data, human resources and labor data, information concerning competitors, customers, and suppliers, market projections, and other information the business relies on to make decisions and operate on a day-to-day basis. Operational data may also include workflows and processes employed by a business.

CATEGORY	DESCRIPTION
Structured Data	Structured data is raw data that is stored in a data platform (a database) that organizes the raw data points in a meaningful way and enables the user to generate reports summarizing the underlying digital information. The database may be commercially available (off the shelf), entirely custom-built, or a hybrid of the two. The usefulness and value of structured data relies on access to the database that organizes and reports on the underlying information.
Unstructured Data	Unstructured data is data lacking a designated pattern and may be considered as a subset of the other classifications. Unstructured data is often difficult to value and may include images, files, and text documents. Typically, unstructured data derives value from further processing and analysis.

CATEGORY	DESCRIPTION
Personally Identifiable Information (PII)	PII is defined by the National Institute of Standards and Technology (NIST) as "(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[37] Common examples of PII include names (e.g., full name, alias, maiden name), personal identification numbers (e.g., driver's license number, financial account number, credit card number), addresses (e.g., street address, workplace, email address), or personal characteristics (e.g., facial images, fingerprints, handwriting).

37. U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., COMPUT. SEC. DIV., SPECIAL PUBL'N 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (April 2010), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. To "distinguish" an individual means to identify an individual (e.g., name, passport number, social security number, biometric information). To "trace" an individual means to process sufficient information to make a determination about a specific aspect of an individual's activities or status (e.g., an audit log of an individual's recorded actions). And "linked" information means information about or related to an individual that is logically associated with other information about the individual (e.g., data from two different access-controlled databases), versus "linkable" information that is about or related to an individual for which there is a possibility of logical association with other information about the individual (e.g., data from one access-controlled database can be paired with information from an unrelated system, such as a public information database).

Particular Types of Data

I. Healthcare

A. Qualifying Data

- Qualifying data in this category includes: individually identifiable health information, Protected Health Information, and Electronic Protected Health Information.

- "'Individually identifiable health information' means any information, including demographic information collected from an individual, that: (A) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and [either] (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."[38]

- "Protected Health Information" (PHI) means individually identifiable health information, that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium, with certain exclusions for education and employment

38. 42 U.S.C. § 1320d(6).

records.[39] "Electronic Protected Health Information" (ePHI) means "electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity."[40]

B. Entities Covered

- Health Insurance Portability and Accountability Act (HIPAA) applies to covered entities and business associates. Covered entities are health plans, healthcare clearinghouses, and healthcare providers.[41] A business associate is a person or entity that uses PHI to perform certain functions or services on behalf of the covered entity.[42]

C. Applicable Laws

- HIPAA prohibits the unauthorized disclosure of PHI by covered entities to certain third parties.[43] The Health Information Technology for Economic and Clinical Health (HITECH) Act extends criminal enforcement and civil liability to covered entities and business associates who, without

39. 45 C.F.R. § 160.103.

40. 45 C.F.R. § 164.105(a)(2)(i)(D).

41. 45 C.F.R. § 160.103.

42. *Id.*

43. *See* 45 C.F.R. § 164.502(e); a broader set of guidelines and rules established by the U.S. Department of Health and Human Services must also be consulted.

authorization, obtain or disclose PHI.[44] Furthermore, the U.S. Department of Health and Human Services (HHS) promulgated (i) the HIPAA Privacy Rule, which establishes national standards for the protection of PHI, and (ii) the HIPAA Security Rule, which requires a national set of security standards for the confidentiality, integrity, and availability of ePHI that an entity creates, receives, maintains, or transmits. The recently issued Omnibus Final Rule expands the definition of "business associate" to generally any entity that creates, receives, maintains, or transmits PHI on behalf of a covered entity (e.g., subcontractors, health information organizations, electronic medical records vendors) and sets both permissible uses of and security requirements for PHI by business associates, as well as defining liability for impermissible use—i.e., business associates are directly liable for impermissible uses and disclosure of PHI.[45] Moreover, under the Final Rule, business associates must conduct a risk analysis of any potential security risks and vulnerabilities to ePHI.

- HIPAA preempts state law only when state law is less stringent.[46] For example, HHS' rules do not restrict the use or disclosure of de-identified health information; however, state laws vary widely in

44. *See* 42 U.S.C. §§ 17935, 17939.; *see also* Kara J. Johnson, *HITECH 101*, AM. BAR ASS'N (June 5, 2012), http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/hitech_101.html.

45. *See* 45 C.F.R. §§ 160, 164.

46. *See* 45 C.F.R. § 160.203(b).

their level of protecting de-identified health information.

D. M&A Impacts

- In healthcare M&A transactions, entities can disclose only the minimum PHI necessary to complete the transaction.[47] Healthcare audits are common, and it is important to consider appropriate security, technical, and physical safeguards early in the M&A process. Parties should analyze all business associate agreements. Business associates that operate under a patient authorization, instead of a business-associate agreement, can incur liability to the target company and the potential buyer because a covered entity cannot rely on patient authorization forms to transfer data when what is required is a business-associate agreement.

- Accordingly, a thorough HIPAA due-diligence review should determine: (i) the type of health information (e.g., PHI and ePHI) collected by the target; (ii) who the target discloses that health information to; (iii) how the health information is transferred to any third parties; and (iv) the target's policies and agreements relating to such information. Representations and warranties that drive the disclosure of these categories of information are highly recommended.

47. *See* 45 C.F.R. § 164.502(b).

II. Biometric Data

A. Qualifying Data

- Biometric data typically refers to either (i) measurable human biological and behavioral characteristics that can be used for identification, or (ii) the automated methods of recognizing an individual based on those characteristics. Examples include facial images, fingerprints, and retinal scans.[48] Many jurisdictions have varying definitions of biometric data, so parties should carefully analyze the rules with respect to the jurisdictions to which they are subject.

B. Entities Covered

- Any entity that collects, processes, or retains biometric data will likely be subject to the additional requirements that attach to biometric data. In practice, the industries most likely to have biometric data include life sciences, pharmaceutical, and medical companies, along with healthcare and technology companies. However, some employers now collect biometric data on their employees, potentially expanding the scope of industries subject to these concerns dramatically.

C. Applicable Laws

- Any entity that collects, processes, or retains biometrics should consult both federal agency

48. Michael P. Daly et al., *Biometrics Litigation: An Evolving Landscape*, PRAC. L. THE J. (April/May 2016).

guidance (e.g., the FTC and the Equal Employment Opportunity Commission (EEOC)) and state laws regarding its security and privacy—recognizing that the regulatory landscape around biometrics is quickly evolving. While biometric data lacks a federal regulatory framework, state laws have raised increased scrutiny of biometric data protection (e.g., in Illinois biometric data is considered to be PII); however, there is heavy debate around what qualifies as a biometric identifier. Illinois's Biometric Information Privacy Act was the first in the country to consider biometric identifiers in a commercial setting; it defines "biometric identifier" as "a retina or iris scan, fingerprint, or scan of hand or face geometry," specifically excluding physical descriptions or photographs.[49] Similarly, in Texas the Capture or Use of Biometric Identifier statute defines "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry," with no specific exclusions to physical descriptions, but excludes photographs or information derived from a photograph.[50] In other states, many healthcare organizations consider it

49. 740 ILL. COMP. STAT. 14/10; *see* 740 ILL. COMP. STAT. 14/20 (noting that statute creates a private right of action for "any person aggrieved" by violation of statute, providing for statutory damages of $1,000 for negligent violation, up to $5,000 for intentional or reckless violation, along with attorneys' fees and costs under 740 ILL. COMP. STAT. 14/20).

50. TEX. BUS. & COM. CODE ANN. § 503.001(a); *see* TEX. BUS. & COM. CODE ANN. § 503.001(d) (noting no private rights of action under statute, but civil penalties can be brought by Texas Attorney General for up to $25,000 per violation).

best practice to engage in heightened security practices when dealing with biometrics.

- The rapid rise in private-sector biometric technology use has been seen not only in technology services (such as facial recognition software used in social media tagging), but also with health and fitness tracking devices (such as smartwatches and apparel). The major concern with this type of data is that unlike passwords or personal identification numbers (PINs), individuals generally cannot change their biometric features, and thus may not prevent access in the case of a data breach. The use of biometric screening has been part of heavy federal privacy scrutiny by the FTC and EEOC where it involves consumer recognition and screening tests that are deemed unfair or deceptive practices under Section 5 of the Federal Trade Commission Act, or are otherwise in violation of the Americans with Disabilities Act.[51] The area has been the subject of increased class-action litigation.[52]

D. M&A Impacts

- Parties to an M&A transaction need to recognize whether biometrics are collected from a product or service offering, or have been stored and retained in the standard course of business (e.g., for internal access control security and employee or customer data). As class-action activity for breaches of biometric data picks up, potential

51. Daly et al., *supra* note 48.

52. *Id.*

liability exposure can be far reaching and expensive. And privacy and security requirements for the collection and retention of biometrics are ever-evolving, so it is important in the due-diligence phase to keep up with regulatory and jurisdiction-specific requirements.

III. Financial Data

A. Qualifying Data

- Qualifying data in this category includes: Non-public Personal Information (NPI), Federal Tax Information (FTI), and Cardholder Data. "NPI" means personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.[53] "FTI" includes any return or return information received from the Internal Revenue Service (IRS) or secondary sources, such as the Social Security Administration, Federal Office of Child Support Enforcement, or Bureau of Fiscal Service, by a state, county, or municipal agency or a contractor providing services to such an agency.[54] FTI includes any information, including PII, created by the recipient that is derived from return or return

53. 15 U.S.C. § 6809(4); Federal Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62,890, 62,892 n.18 (Dec. 1, 2009).

54. *See* INTERNAL REVENUE SERV., PUBL'N 1075, TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES (Sept. 2016), https://www.irs.gov/pub/irs-pdf/p1075.pdf [hereinafter IRS Pub. 1075].

information.[55] "Cardholder Data" includes the primary account number, cardholder name, expiration date, and service code; "Sensitive Authentication Data" includes "full track data" (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, PINs/PIN blocks; "Cardholder Data Environment" is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data; and "System Components" includes network devices, servers, computing devices, and applications (e.g., Domain Name System (DNS) servers, network firewalls, and virtual machines).[56]

B. Entities Covered

- Numerous entities are subject to the rules covering the data protection and privacy of financial data. The primary entities subject to these rules are financial institutions. "Financial institutions" refers broadly to companies that are "engaging" in offering financial products or services to individuals, like loans, financial or investment advice, or insurance, but excludes certain entities (e.g., those subject to the Commodity Futures Trading Commission).[57] Also, companies that

55. *See id*.

56. PAYMENT CARD INDUS. SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES (version 3.2.1 May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1557430674216 (hereinafter PCI DSS Version 3.2.1).

57. *See, e.g.*, 15 U.S.C. § 6809(3); 15 U.S.C. § 6801.

provide support to state or local governments that include the handling or processing of Federal Tax Information will likely be subject to the rules covering financial data.

- In addition, companies that in any way handle credit card information are subject to the Payment Card Industry Data Security Standard (PCI DSS). Specifically, PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data or sensitive authentication data, and to entities that accept credit cards or otherwise use credit card data. Note that PCI DSS may also apply to payment application vendors if the vendor stores, processes, or transmits cardholder data, or has access to such cardholder data.[58]

C. Applicable Laws

- The data protection and privacy of financial information have long been subject to a variety of federal, state, and industry-based statutes, rules, and guidelines, involving everything from the encryption of data to privacy disclosures to consumers under the Gramm-Leach-Bliley Act (GLBA). GLBA limits how financial institutions use specific types of NPI from consumers—i.e., their information-sharing practices.[59] Under the GLBA's

58. *See* PCI DSS Version 3.2.1, *supra* note 56.

59. 15 U.S.C. §§ 6801–6809.

Financial Privacy Rule, a financial institution may only disclose consumers' NPI in connection with a sale, merger, or transfer of a business with affiliated third parties.[60] "Customers" (consumers who are in a customer relationship with the institution) must be provided a reasonable opportunity to direct the financial institution not to share NPI about them (i.e., an opt-out) with non-affiliated third parties other than as permitted by the statute (e.g., for everyday business processing purposes or as part of government requests).[61]

- The privacy of NPI also translates to compliance with the Fair Credit Reporting Act (FCRA), more broadly. The FCRA applies to entities that use credit reporting agencies to determine a person's credit worthiness, character, mode of living, or general reputation.[62] It mandates that companies provide policies to reasonably ensure consumers of accurate data, and provides a reasonable process for consumers to correct inaccurate information.[63] Some state laws also establish stringent privacy standards, such as California's Financial Information Privacy Act, which requires affirmative consent from consumers for companies to share certain information with affiliated parties.[64]

60. 15 U.S.C. § 6802(e)(7).

61. *See* Federal Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. at 62,892.

62. *See* 15 U.S.C. § 1681.

63. *See* 15 U.S.C. § 1681b.

64. *See* CAL. FIN. CODE §§ 4050–4060.

- The GLBA further outlines how financial institutions must safeguard NPI. The GLBA's Safeguards Rule makes specific financial regulatory agencies, such as the FTC, responsible for establishing standards "relating to administrative, technical, and physical safeguards (i) to insure the security and confidentiality of customer records and information; (ii) to protect against any anticipated threats or hazards to the security or integrity of such records; and (iii) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[65] It should be noted that the Safeguards Rule (i) is applicable to entities that are not subject to the Privacy Rule (e.g., student loan operators), and (ii) requires that specific confidentiality and security requirements are met when handling NPI (e.g., having a written information security plan).[66]

- Notably, encryption standards are often required for handling certain financial data. The IRS has issued security controls under I.R.C. § 6103 for tax returns that involve FTI.[67] The IRS similarly provides guidance on how certain entities collecting FTI can comply with respect to email, data

65. 15 U.S.C. § 6801(b).

66. *See Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (April 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

67. *See* IRS Pub. 1075, *supra* note 54.

transfers, mobile devices, and databases.[68] Similarly, the Financial Industry Regulatory Authority (FINRA) issues rules for financial institutions to comply with Security and Exchange Commission regulations by adopting written policies and procedures to protect customer information, defining duties to conduct information security operations, and preserving electronically stored records using encryption.[69] FINRA has been active in bringing enforcement actions against financial institutions that do not adopt encryption standards.[70] Similarly, certain states have their own data encryption laws for financial data, which also implicate state-level data-breach statutes. State Attorneys General often impose heavy penalties if a data breach is not properly disclosed.[71]

---

68. *See Encryption Requirements of Publication 1075*, INTERNAL REVENUE SERV., https://www.irs.gov/uac/encryption-requirements-of-irs-publication-1075 (last updated Jul. 18, 2018).

69. *See, e.g.*, *Cybersecurity*, FIN. INDUS. REG. AUTH., http://www.finra.org/industry/cybersecurity (last visited May 9, 2019).

70. FINRA recently brought an enforcement action against a broker-dealer that lost a laptop with unencrypted consumer data, ordering it to pay fines, even without a showing of a known identity theft or customer financial loss. *See* Jody Godoy, *Sterne Agee Settles With FINRA Over Laptop Privacy Breach*, LAW360 (May 26, 2015, 3:57 P.M.), http://www.law360.com/articles/659794/sterne-agee-settles-with-finra-over-laptop-privacy-breach ("[T]he firm failed to take appropriate technological precautions to protect customer and highly sensitive information[.] . . . There were no [written security protocols] to ensure that the firm's most sensitive customer and proprietary information stored on laptops were being adequately safeguarded by appropriate technology, such as encryption." (final alteration in original)).

71. *See, e.g.*, LB835, 104 Leg., 2d Sess. (Neb. 2016).

- Entities that process financial data through payment systems, both within a brick-and-mortar and online retail setting, must follow certain industry-based guidelines. The Payment Card Industry Security Standards Council issues the PCI DSS, which requires that all entities that process, store, or transmit Cardholder Data or Sensitive Authentication Data maintain a secure Cardholder Data Environment. PCI DSS version 3.2 was published in April 2016 and calls for stronger encryption standards and multifactor authentication.[72]

D. M&A Impacts

- Several financial laws, regulations, and industry guidelines can affect an M&A transaction in the privacy and data security context. Target companies should have standards and written policies in place that comply with the GLBA's Financial Privacy Rule governing NPI, as well as any rules established by an appropriate financial regulatory agency, including states, and, where applicable, must be mindful of the FCRA. The processing of FTI and payment data must undergo further scrutiny both during and after an M&A transaction. Buyers should insist on very robust representations driving the disclosure of all agreements and data pertaining to these data types.

72. *See* PCI DSS Version 3.2.1, *supra* note 56.

IV. Energy Data

A. Qualifying Data

- Qualifying data in this category includes "Bulk Electric System Cyber Information," which means "information about the BES [Bulk Electric System] Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System."[73] For example, this would include security procedures or information about the BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that are not publicly available and could be used to allow unauthorized access or unauthorized distribution. It would exclude pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Systems, such as device names, individual IP (Internet Protocol) addresses without context, ESP (Electronic Security Perimeter) names, or policy statements.

- Note the following definitions. "BES Cyber System" means "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity."[74] "BES Cyber Asset" relates to any "Cyber Asset that if rendered unavailable,

---

73. *Glossary of Terms Used in NERC Reliability Standards*, N. AM. ELEC. RELIABILITY CORP. (Mar. 8, 2019), http://www.nerc.com/files/glossary_of_terms.pdf.

74. *Id*.

degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the [BES]."[75] "Cyber Asset" means "[p]rogrammable electronic devices, including the hardware, software, and data in those devices."[76]

B. Entities Covered

- The entities and industries most likely to be concerned with this category of data include electric utilities and energy producers. More specifically, these entities include Bulk Electric Systems and other entities subject to Federal Energy Regulatory Commission (FERC) regulation.

C. Applicable Laws

- With rising concerns over critical infrastructure protection and electric grid reliability, energy producers and utilities, in general, are subject to a variety of FERC (or the U.S. Nuclear Regulatory Commission (NRC)) and industry-based guidelines regarding their data and industrial control systems. Recently, FERC issued a final rule adopting seven revised Critical Infrastructure Protection (CIP) Reliability Standards and physical

75. *Id*.

76. *Id*.

controls addressing cybersecurity.[77] Industry guidelines to comply with these rules have been developed by the North American Electric Reliability Corporation (NERC) regarding CIP Reliability Standards and have been approved by the FERC.[78] Facilities regulated by the NRC, however, follow their own set of cybersecurity rules particular to nuclear considerations.[79]

D. M&A Impacts

- Data involving a BES Cyber System is considered part of critical infrastructure. M&A due diligence should consider whether a target electric, nuclear, or other energy-producing company complies with the security protocols promulgated by the

77. The seven reliability standards are: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection). Revised Critical Infrastructure Protection Reliability Standards, 81 Fed. Reg. 4,177, 4,177 (Jan. 26, 2016).

78. *See Cyber Security Standards Transition Guidance*, N. AM. ELEC. RELIABILITY CORP. (Apr. 11, 2013), https://www.nerc.com/pa/comp/Resources/ResourcesDL/Cyber_Security_Standards_Transition_Guidance.pdf.

79. *See* 10 C.F.R. § 73.54; *NRC Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities*, U.S. NUCLEAR REG. COMM'N (Jan. 2010), http://www.nrc.gov/docs/ML0903/ML090340159.pdf. The NRC uses the following terms: "critical digital asset" (CDA) to mean "[a] subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network;" "critical system" (CS) means "[a]n analog or digital technology based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function[,]" (e.g., equipment, communication systems, networks). *Id.* at 35.

FERC, NRC, or any other specially commissioned industry group. Acquiring entities should be sure they understand the compliance footing of the acquired entity because coming into compliance may be a significant liability that could impact the economic return of the transaction.

V. Telecommunications Data

A. Qualifying Data

- Qualifying data in this category includes "Customer Proprietary Network Information" (CPNI). CPNI includes customers' telephone call-detail records and logs, network subscription and services, and other subscriber information used for billing.[80]

B. Entities Covered

- The entities most traditionally concerned with this category of data were telecommunications carriers. Increasingly, however, the entire mobile industry, including hardware and software companies and internet service providers (ISPs), are concerned with this data set.

C. Applicable Laws

- Traditionally, only telecommunications carriers were subject to Federal Communications Commission (FCC) regulations, mostly regarding CPNI privacy. But as the FCC becomes more

80. 47 U.S.C. § 222(h)(1); *see* 47 C.F.R. §§ 64.2001–.2011.

active in regulating mobile networks—often overlapping with FTC jurisdiction—its regulatory reach has also expanded to include the scrutiny of privacy and security of the broader industry (e.g., smartphone manufacturers). Traditional carriers have long been subject to privacy rules over certain data that they collect from customers. Under the Telecommunications Act, the FCC is tasked with regulating how telecommunications companies collect, use, and share CPNI that includes customers' telephone call-detail records and logs, network subscription and services, and other subscriber information used for billing.[81]

- The FCC recently promulgated rules to protect broadband consumer privacy—a step that expands the FCC's reach from phone carriers to include ISPs, along with smartphone hardware and software companies.[82] The rules deal largely with how ISPs collect and use information regarding their customers' online activities. They also establish cybersecurity requirements for how ISPs protect CPNI among other types of information, including the implementation of risk management practices and audits.[83] For example, the FCC and FTC have initiated parallel regulatory

81. *See* 47 C.F.R. § 64.2001–.2011.

82. *See FCC Releases Proposed Rules to Protect Broadband Consumer Privacy*, FED. COMMC'NS COMM'N, https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy (last visited May 9, 2019).

83. *See* Press Release, Fed. Commc'ns Comm'n, FCC Proposes to Give Broadband Consumers Increased Choice, Transparency and Security for Their Personal Data (March 31, 2016), https://docs.fcc.gov/public/attachments/DOC-338679A1.pdf.

assessments into mobile security risks and vulnerabilities.

D. M&A Impacts

- While parties to an M&A transaction involving telecommunications carriers are required to comply with the FCC's privacy guidance, companies whose practices may touch on telecommunication issues as part of their core or ancillary practices may need to consider the FCC's emerging role in setting additional privacy and security standards. An acquirer should be aware that by purchasing one of these companies, it could end up entering a world of regulation with which they are unfamiliar.

APPENDIX B:
SAMPLE REPRESENTATIONS AND WARRANTIES

In an information economy, it is increasingly important to understand the information security and privacy protections that target companies across industries have in place at the time of an acquisition, whether in a stock deal or asset purchase. Traditionally, representations and warranties relating to information security and privacy have been "flat," meaning they make a general statement about the acquired assets or business that is required to be true. The parties then negotiate over the language of the representation or warranty, adding or subtracting qualifiers such as knowledge, duration of time, and materiality. Because we believe that the information practices and procedures of companies and their compliance with a myriad of industry-specific laws, regulations, and guidelines require a more nuanced approach, we provide sample representations and warranties focused on driving disclosure where practicable.

These sample representations and warranties are for use in an acquisition and adopt disclosure-focused schedules detailing the seller's practices, policies, and third-party contracts, along with the type of data that it collects, uses, or discloses subject to the transaction. Below are nine critical areas in an acquisition, with examples and recommended disclosure provisions: (1) Compliance with Information Security and Data Privacy Laws; (2) Information Security Measures and Standards; (3) User Privacy and Information Security Policies;[84] (4) Information Security and Data Privacy Third-Party Contractual Obligations; (5) Data Access Policies; (6) Information Security and Data Privacy Complaints and Investigations; (7) Security Breaches and Unauthorized Use of Personal Information; (8) Effect of the Transaction on Personal Data; and (9) Cybersecurity Insurance.

84. This provision relates to both consumer data and employee data.

The following sample representations and warranties are neutral in nature and should be modified, where applicable, to align with the buyer's interests. These provisions are not industry-specific and are drafted to work for a broad range of companies. Accordingly, they may need to be modified depending on the industry in which the target business operates. Where appropriate, counsel should consult with industry specialists to ensure relevant industry concerns and issues are adequately addressed.

1. Compliance with Information Security and Data Privacy Laws.

a. Sample contractual language:

i. Compliance with Laws. Except as set forth on Schedule [ ], the Company is and for the past [ ] years has been in compliance, in all material respects, with all (i) Information Security and Data Privacy Laws, and (ii) Foreign Information Security and Data Privacy Laws.

b. Pertinent defined term(s):

i. "Information Security and Data Privacy Laws" means the following laws, to the extent applicable to the Company and solely to the extent related to the collection, use, disclosure, and protection of personal data: (a) the Fair Credit Reporting Act (FCRA) of 1970, as amended; (b) the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM); (c) the Privacy Act of 1974, as amended; (d) the Family Educational Rights and Privacy Act (FERPA) of 1974, as amended; (e) the Right to Financial Privacy Act of 1978, as amended; (f) the Privacy Protection Act of 1980, as amended; (g) the Cable Communications Policy Act of 1984, as

amended; (h) the Electronic Communications Privacy Act (ECPA) of 1986, as amended; (i) the Video Privacy Protection Act (VPPA) of 1988, as amended; (j) the Telephone Consumer Protection Act (TCPA) of 1991, as amended; (k) the Driver's Privacy Protection Act of 1994, as amended; (l) the Communications Assistance for Law Enforcement Act of 1994, as amended; (m) the Telecommunications Act of 1996, as amended; (n) the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended; (o) the Children's Online Privacy Protection Act (COPPA) of 1998, as amended; (p) the Financial Modernization Act (Gramm-Leach-Bliley Act (GLBA)) of 2000, as amended; (q) state laws governing the use of electronic communications, e.g., email, text messaging, telephone, paging, and faxing; (r) state laws governing the use of information collected online, state laws requiring privacy disclosures to consumers, state data-breach notification laws, state laws investing individuals with rights in or regarding data about such individuals and the use of such data, and any state laws regarding the safeguarding of data, including encryption; and (s) any relevant federal or state guidelines or recommended best practices for information security and data privacy, including, but not limited to, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and Federal Trade Commission (FTC) privacy guidelines.[85]

85. The defined term of Privacy Laws listed above provides myriad privacy-related laws that may apply to a host of regulated industries. Parties to

ii. "Foreign Information Security and Data Privacy Laws" shall mean (a) the Directive 95/46/EC of the Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the collection, use, disclosure, and processing of personal data and on the free movement of such data and any other applicable laws relating to the processing of personal data, including Directive 2002/58/EC as amended and all related regulations, regulatory codes of practice and guidance issued from time to time, including from the European Commission, and other relevant data protection supervisory authorities; (b) the corresponding national rules, regulations, codes, orders, decrees, and related rulings of the member states of the European Union; (c) the Personal Information Protection and Electronic Documents Act (Canada) and Canada's Anti-Spam Legislation; and (d) any rules, regulations, codes, orders, decrees, and related rulings concerning personal data and the privacy, data protection, or data-transfer issues regarding the same implemented in Canada or other non-U.S. countries.[86]

---

a transaction are encouraged to customize the Privacy Laws definition to align with their given industry (e.g., healthcare, telecommunications, retail).

86. International law should also be considered when complying with data security laws. Particularly, when transferring data of European Union (EU) citizens, the seller should comply with the European Union Privacy Directive (Directive 95/46/EC) and must comply with model contracts, binding corporate rules, or other standards when transferring personal data outside the EU. Please note that foreign privacy standards as used in cross-border data transfers with the EU are undergoing significant revisions as per the EU-U.S. Privacy Shield Framework.

2. Information Security Measures and Standards.

a. Sample contractual language:

i. Information Security Measures. Schedule [ ] sets forth a true and complete list of the Company's information security and data protection policies, programs, and procedures that: (i) include administrative, technical, personnel, organizational, and physical safeguards designed to protect the security, confidentiality, and integrity of transactions, data, and other information in the Company's Information Systems, and (ii) are designed to protect against unauthorized or unlawful access to the Company's Information Systems and the systems of any third-party service providers that have access to the Information Systems. The Company has at all times been in compliance with the policies, programs, and procedures set forth on Schedule [ ].

b. Pertinent defined term(s):

i. "Information Systems" means the computer software, computer firmware, computer hardware (whether general purpose or special purpose), telecommunications, equipment, controlled networks, peripherals, and computer systems, including any outsourced systems and processes under the Company's control, and other similar or related items of automated, computerized, and/or software systems that are owned, licensed, leased, or controlled by the Company and used or relied on in connection with the Company's business, but excluding the public Internet.

3. User Privacy and Information Security Policies.

a. Sample contractual language:

i. User Privacy Policy. Schedule [ ] sets forth a true and complete list of each of the Company's privacy policies regarding the collection, storage, use, and distribution of Personal Information. Each privacy policy of the Company has commercially reasonable information security and data protection controls in place, consistent with general industry practice based on the type of data and degree of risk associated with Personal Information, designed to protect the security and confidentiality of Personal Information (i) against any threats or hazards to the security and integrity of Personal Information and (ii) against any unauthorized access to or use of Personal Information contrary to this Agreement or any applicable Privacy Laws. The Company is in compliance, in all material respects, with its stated privacy policies set forth in Schedule [ ], and has maintained such compliance, in all material respects, for the past [ ] years.

ii. Information Security Policy. Schedule [ ] contains a true and complete list of all of the Information Systems that are material to the operation of the business of the Company or the business of the Company's customers, not including off-the-shelf products. If such Information Systems are operated or hosted by an outsourcer or other third-party provider, the identity and contact information for the third-party provider is disclosed on Schedule [ ]. None of the Information Systems depend upon any technology or information of any third party (other than the public Internet). Such Information Systems

are sufficient for the conduct of the Company's business as currently conducted and as anticipated to be conducted by the Buyer. The Company uses commercially reasonable means, consistent with industry practice and state of the art technology generally available to the public, to protect the security and integrity of all the Information Systems set forth in Schedule [ ]. As set forth on Schedule [ ], the Company has implemented and maintains information security and data protection policies, programs, and procedures to ensure the security of the Information Systems. Furthermore, the Company's use of the Information Systems does not exceed the scope of the rights granted to the Company with respect to those rights, including any applicable limitation upon the usage, type, or number of licenses, users, hardware, time, services, or systems.

b. Pertinent defined term(s):

   i. "Personal Information" means any information that relates to an identified or identifiable individual, including name, address, telephone number, email address, username and password, photograph, government-issued identifier, persistent-device identifier,

or any other data used or intended to be used to precisely identify an individual.[87, 88]

ii. *See* 2(b)(i), *supra*, for an example definition of "Information Systems."

4. Information Security and Data Privacy Third-Party Contractual Obligations.

a. Sample contractual language:

i. Contractual Compliance. Schedule [ ] sets forth a true and complete list of each agreement and Contract with a third party that provides the Company with consumer data, including privacy policies relating to data privacy, security, or breach notification (including provisions that impose conditions or restrictions on the collection, use, disclosure, transmission, destruction, maintenance, storage, or safeguarding of Personal Information). Schedule [ ] sets forth each Contract in which a Security Breach of the

87. Companies may also handle Personally Identifiable Information (PII). PII is defined by the NIST as being "(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." *Glossary*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/personally-identifiable-information (last visited May 9, 2019). Common examples of PII include names (e.g., full name, alias, maiden name), personal identification numbers (e.g., driver's license number, financial account number, credit card number), addresses (e.g., street address, workplace address, email address), or personal characteristics (e.g., facial images, fingerprints, handwriting).

88. Personal Information relates to both consumer data and employee data. Even for companies that do not possess consumer PII, these representations and warranties will be relevant to any employee data that will be assumed or transferred in connection with a stock or asset purchase.

Information System would result in a material breach of the terms of agreement. Schedule [ ] sets forth each Contract that requires the Company to notify any affected individual in the case of a Security Breach of the Information Systems. The Company is in compliance in all material respects with the terms of each of the Contracts listed on Schedules [ ], [ ], and [ ] and has maintained such compliance, in all material respects, for the past [ ] years. The Company includes in each of its Contracts with third parties that process, store, or otherwise handle Personal Information on behalf of the Company, contractual provisions that the third parties will comply with the Company's Information Security and Data Privacy policies, as set forth in Schedules [ ] and [ ], respectively, and all applicable Information Security and Data Privacy Laws in connection with their activities for the Company[, except as set forth in Schedule [ ], and has included such contractual provisions, in all material respects, for the past [ ] years.

b. Pertinent defined term(s):

   i. "Security Breach" means any act or omission that compromises either the security, confidentiality, or integrity of Personal Information, or compromises the physical, technical, administrative, or organizational safeguards put in place by the Company that relate to the protection of the security, confidentiality, or integrity of Personal Information.
   ii. *See* 1(b)(i) and 1(b)(ii), *supra*, for example definitions of "Information Security and Data Privacy Laws" and "Foreign Information Security and Data Privacy Laws."

iii. *See* 3(b)(i), *supra*, for an example definition of "Personal Information."

5. Data Access Policies.

a. Sample contractual language:

i. Data Access Policies. Schedule [ ] contains a true and complete list of the Company's data-access policies and procedures, setting forth (i) the transit of the Company's data and data flows, including, but not limited to, the Company's network topology, databases, document management systems, and any cross-border data transfers outside of the Territory; (ii) the Company's data-classification system and methodology; (iii) the Company's data collection and retention processes; and (iv) the requirements for granting or revoking access to Personal Information contained in the Company's Information Systems. The Company is currently in compliance with each of the data-access policies and procedures set forth on Schedule [ ] and has maintained such compliance, in all material respects, for the past [ ] years. The Company has taken commercially reasonable steps to protect and maintain the integrity and confidential nature of the Personal Information provided to the Company in reliance on the Company's data-access policies, in all material respects, for the past [ ] years.

b. Pertinent defined term(s):

i. *See* 3(b)(i), *supra*, for an example definition of "Personal Information."

ii. *See* 2(b)(i), *supra*, for an example definition of "Information Systems."

6. Information Security and Data Privacy Complaints and Investigations.

a. Sample contractual language:

i. Information Security and Data Privacy Litigation. Except as set forth in Schedule [ ], to the Company's knowledge, there are no pending or threatened claims, charges, investigations, violations, settlements, civil or criminal enforcement actions, lawsuits, or other court actions against the Company that allege either (i) a material security breach of information security, including, but not limited to, a network intrusion, incident involving the Company's Personal Information, or a data breach of the Company's Information Systems; or (ii) a violation of any Person's privacy, personal, or confidential rights under the Company's information security or data privacy practices, other than those listed in Schedules [ ] and [ ], or any Information Security and Data Privacy Laws.[89]

b. Pertinent defined term(s):

i. *See* 3(b)(i), *supra*, for an example definition of "Personal Information."
ii. *See* 2(b)(i), *supra*, for an example definition of "Information Systems."
iii. *See* 1(b)(i) and 1(b)(ii), *supra*, for example definitions of "Information Security and Data Privacy Laws"

89. In the event that a known material issue exists, buyers may require a purchase-price adjustment or, alternatively, a line-item indemnity. *See* Sections IV(B)–(C), *supra,* for a discussion on those considerations. The magnitude and severity of any identified issues will dictate whether a purchase-price adjustment or a special indemnity is a more suitable risk-shifting alternative.

and "Foreign Information Security and Data Privacy Laws."

7. Security Breaches and Unauthorized Use of Personal Information.

a. Sample contractual language:

i. Unauthorized Access and Security Breaches. To the Company's knowledge, and except as set forth on Schedule [ ], there has been no breach of the Information Systems or security of any personally identifiable or confidential data, including any unauthorized access to, acquisition of, disclosure of, or loss of data possessed or controlled by the Company, except in each case as would not, individually or in the aggregate, reasonably be expected to have a Material Adverse Effect, and the Company has not received any written notices or complaints from any Person with respect to any breach.

b. Pertinent defined term(s):

i. *See* 2(b)(i), *supra*, for an example definition of "Information Systems."

8. Effect of the Transaction on Personal Data.

a. Sample contractual language:

i. Effect of the Transaction. Neither (i) the execution, delivery, or performance of this Agreement, (ii) the consummation of any of the transactions contemplated by this Agreement (or any of the other ancillary agreements), nor (iii) the Buyer's possession or use of the Personal Information or any data or information in the Company's possession, will result in any breach or violation of any internal privacy

policy of the Company [as listed in Schedule [ ]], Contract [as listed in Schedule [ ]], or any Information Security and Data Privacy Laws pertaining to the collection, use, disclosure, transfer, or protection of Personal Information, except in each case as would not, individually or in the aggregate, reasonably be expected to have a Material Adverse Effect. Upon the Closing of this Transaction, the Buyer will continue to have the right to use such Personal Information on identical terms and conditions as the Company enjoyed immediately prior to the Closing.[90]

b. Pertinent defined term(s):

i. *See* 3(b)(i), *supra*, for an example definition of "Personal Information."

ii. *See* 1(b)(i) and 1(b)(ii), *supra*, for example definitions of "Information Security and Data Privacy Laws" and "Foreign Information Security and Data Privacy Laws."

9. Cybersecurity Insurance.

a. Sample contractual language:

i. Insurance. Schedule [ ] sets forth a true and complete list of all current policies or binders of fire, liability, workers' compensation, property, casualty, errors and omissions, employment practices, crime,

90. To ensure compliance with this representation, the parties should consider whether any constraints on the target company's ability to transfer the data exist. Constraints will often be in the form of pre-existing contractual restrictions and found in the target company's existing privacy policies. Even if the target company has valid ownership rights to certain data, the buyer may not have unrestricted use of—or transferability rights to—that data.

cybersecurity, and other forms of insurance owned or held by the Company (collectively, the "Insurance Policies"). True and complete copies of the Insurance Policies have been made available to the Buyer. The Insurance Policies are in full force and effect. The Company has not received any written notice of cancellation of, premium increase with respect to, or alteration of coverage under any of the Insurance Policies. All premiums due on the Insurance Policies have either been paid or, if due and payable prior to Closing, will be paid prior to Closing in accordance with the payment terms of each Insurance Policy. All of the Insurance Policies (a) are valid and binding in accordance with their terms; (b) are, to the Company's knowledge, provided by carriers who are financially solvent; and (c) have not been subject to any lapse in coverage. There are no claims related to the business of the Company pending under any of the Insurance Policies for which coverage has been questioned, denied, or disputed, or for which there is an outstanding reservation of rights. The Company is not in default under, nor has it otherwise failed to comply with, in any material respect, any provision contained in any Insurance Policy. The Insurance Policies are of the type and in the amounts customarily carried by Persons conducting a business similar to the Company, and are sufficient for compliance with all applicable Laws, including Information Security and Data Privacy Laws and Contracts to which the Company is a party or by which it is bound.

b. Pertinent defined term(s):

i. *See* 1(b)(i) and 1(b)(ii), *supra*, for example definitions of "Information Security and Data Privacy Laws" and "Foreign Information Security and Data Privacy Laws."

APPENDIX C:
DUE-DILIGENCE REQUESTS

In connection with the potential acquisition and subject to the mutual nondisclosure agreement, please provide us with the following materials. If certain materials have already been provided, are unavailable, or are generally inapplicable, please indicate so in your response to this request. Please note that our due-diligence investigation is ongoing, and we will submit supplemental due-diligence requests as necessary.

Unless otherwise indicated, any responsive documents should be made available for all periods subsequent to [DATE] and should include all amendments, supplements, or other ancillary documents.

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
I. Data		
a. Describe and identify the location of: i. Consumer PII ii. Employee PII iii. Financial information iv. HIPAA data v. Aggregated/de-identified consumer information		
b. Identify and generally describe trade secret information and other proprietary know-how.		
c. List and describe databases material to the organization.		
d. List and describe other data repositories.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
II. Hardware		
a. List and describe all in-house servers, Network Attached Storage (NAS) document management systems, data warehouses, and other hardware and computing assets belonging to the organization.		
b. List and describe all owned personal computers.		
c. List and describe encryption technologies employed on owned hardware.		
d. Provide details of any plans for significant software or IT systems upgrades within the next 12 months, indicating for each planned upgrade the status of completion or negotiation of related agreements and an estimate of the associated capital expenditures.		
e. Provide details of any material failures or interruptions in the use of the organization's IT systems in the past 12 months, indicating for each item the status of remediation and the actual or anticipated impact on the organization's business.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
III. Software		
a. Provide a list describing all proprietary technology and computer software owned or being developed by or for the organization.		
b. Provide a list describing all: i. material third-party computer software used by the organization or incorporated into any software or product of the organization; and ii. open-source, freeware, or other software having similar licensing or distribution models used by the organization or incorporated into any software or product of the organization.		
c. Provide details (and copies where available) of material support agreements relating to the organization's software/hardware (including maintenance, disaster recovery, and outsourcing arrangements).		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
d. Provide details of any significant errors or performance issues experienced by the organization in the previous 12 months in connection with the organization's software/hardware, and steps that the organization has taken to resolve those errors or performance issues.		
e. Provide copies of all agreements relating to the provision of IT, data, or internet-related products or services to or by the organization.		
IV. Policies		
a. Describe the organization's collection, use, transmission, storage, or disposal of personal, financial, and health information of its customers or other individuals.		
b. Provide copies of all current and historical privacy and data protection, retention, storage, classification, destruction, or security policies and practice manuals of the organization, including, without limitation, all privacy policies and procedures for the organization's use and disclosure of customer/client or personal information.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
c. Provide details of any training that is given to the employees on data protection, and the appointment of data protection officers.		
d. Provide copies of any other documentation and information regarding the organization's collection, use, storage, or disposal of customer or personal information.		
e. Describe and furnish copies of the organization's trade-secret policies and the measures taken to protect trade secrets and proprietary know-how.		
f. Provide details of any backup, business-continuity, and disaster-recovery plans and procedures, facilities management, and ongoing support arrangements.		
g. Provide copies of customer-facing website privacy policies and terms of use.		
h. Provide copies of all current and historical breach notification and response plans and procedures.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
V. Agreements; Vendors		
a. Provide copies of all agreements that the organization has with any service providers and other vendors that (i) receive from or on behalf of the organization any customer or personal information that is subject to any data privacy or security requirements, or (ii) have access to the organization's networks.		
b. List and describe all hosting, cloud-computing, or collaboration services.		
c. Provide details regarding any data processor appointed by the organization and copies of all such agreements.		
d. Provide details of any agreements under which the organization has been appointed a data processor and copies of any applicable agreements.		
e. Provide details of any agreements entered into by the organization or its subsidiaries relating to the transfer of personal data out of the European Economic Area.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
f. Provide copies of all agreements that the organization has with any third parties that act as the organization's agents or contractors and that receive customer or personal information subject to any statutory or regulatory data privacy or security requirements from or on behalf of the organization. Please provide copies of any reports or audits (internal or external, and including any SAS 70 and SSAE 16 audits) that have been performed on the information security program(s) of such third parties.		
VI. Litigation; Enforcement		
a. List and describe (including an estimate of the amount of the organization's contingent liability) any claims, charges, arbitrations, grievances, actions, suits, investigations, or proceedings involving the IT or data assets of the organization or its affiliates in connection with the organization currently outstanding, outstanding at any time within the last five (5) years, or pending, threatened, or contemplated.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
b. List, describe, and provide a copy of all unsatisfied or outstanding judgments, writs, injunctions, decrees, awards, or orders of any court or other governmental agency or body relating to or affecting the IT or data assets of the organization.		
c. Provide a summary of all reports to and correspondence with governmental agencies involving the data of the organization.		
d. Provide copies of all of the organization's notifications to and requests for authorization from the relevant supervisory authority under applicable national data protection law.		
e. Provide details of any complaints, notices, or other correspondence relating to the organization from the relevant national supervisory authority or any other party in relation to data protection, and copies of all material correspondence.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
f. Provide details of any audits or investigations (internal or external, including any SAS 70 and SSAE 16 audits) relating to the information security practices of the organization (or any service providers or other vendors that receive customer or personal information from or on behalf of the organization), and copies of any reports prepared by or for the organization concerning the implementation of information security program(s) by the organization or such service providers or other vendors.		
g. Provide details of any complaints, claims, proceedings, or litigation relating to the organization's information security practices, and copies of any notices, pleadings, correspondence, or other relevant documents.		
h. Provide details of any actual or potential data and information security breaches, unauthorized use or access of the organization's IT systems or data, or data and information security issues affecting the organization in the past 5 years.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
i. Provide details of any actual or potential hacking, viruses, or other attacks on the organization's websites or social media sites in the past 5 years, indicating for each item the status of remediation and the actual or anticipated impact on the organization's business.		
j. Describe any insurance coverage for business losses related to the organization's computer systems.		
k. List and describe any known lapses in insurance coverage or insurance claims made or pending with respect to the insurance policies relating to the organization's computer systems.		