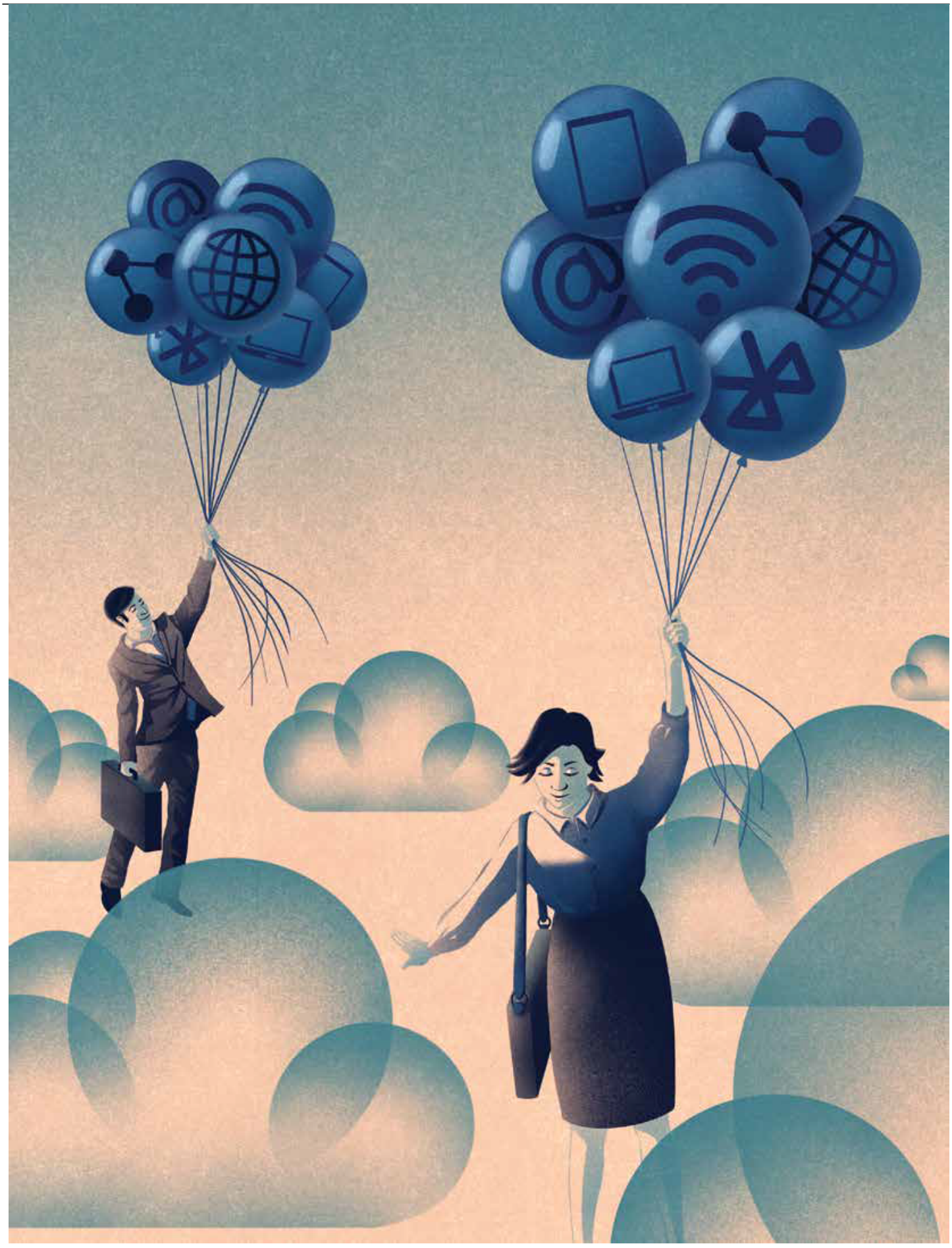
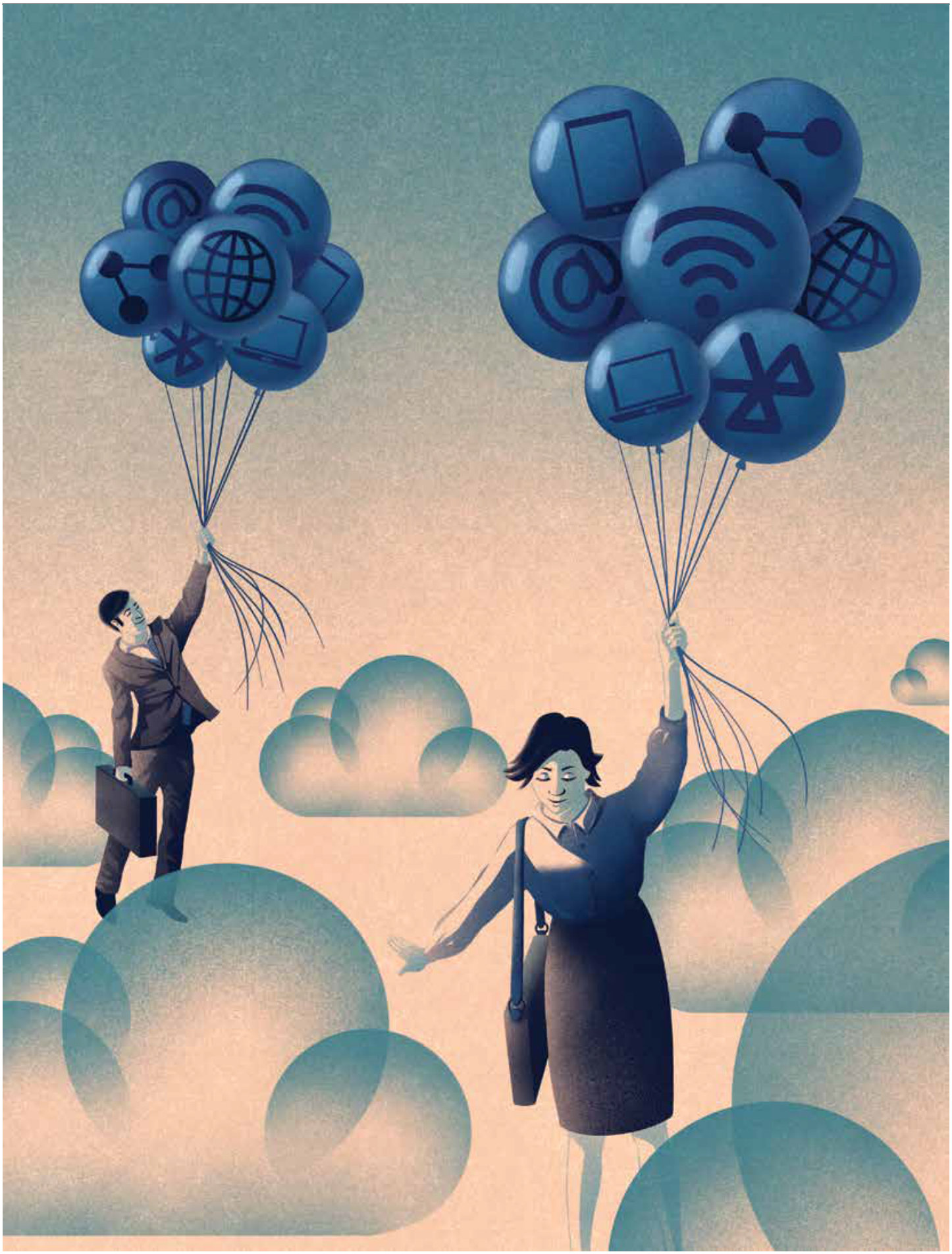
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Parting the Clouds of Digitalization

Technology, Privacy, and eCommerce





CHEAT SHEET

- ***Be prepared.*** Eighty-one percent of legal departments are not ready for digitalization, meaning issues like cybersecurity and lack of data privacy can pose serious threats to a company's risk management.
- ***Corporate value.*** Data rights, customer trust, and networks are showing a greater need for legal safeguards as they become more valuable assets.
- ***Right to be forgotten.*** Legal forethought must be given to the GDPR's "right to be forgotten" and the right to prohibit sale of personal data when developing digitalization projects.
- ***Reasonable risk.*** Counsel must work with senior leadership and the board of directors to determine their organization's stance on risk tolerance.

Late last year, the global research and advisory firm Gartner released data reporting that the majority of legal departments — 81 percent — are unprepared for digitalization. As digital transformation initiatives surge forward with increasing urgency driven by business needs and IT strategy, digitalization risks, like those related to data privacy, are often an afterthought. Conversely, legal teams that are properly prepared for their organization's digital change can increase on-time digital project delivery by 63 percent and increase the number of digital projects with appropriate risk management measures in place by 46 percent, according to Gartner.

These figures are compelling. When combined with the broader risk mitigation that results from proactive and holistic information governance, this data makes a strong case for why in-house legal departments should prioritize their ability to keep pace with digital transformation initiatives.

Digitalization and regulation

With today's rapidly changing regulatory, information security, and data privacy landscape at local, national, and global levels, it is imperative that legal departments take a proactive effort in understanding the legal risks of digitalization projects and address them before they create potential problems and additional costs for the enterprise and, ultimately, shareholders. Digitalization and the use of technology and data to engage with customers and stakeholders directly is an exploding trend across all industries. Jack Ma, founder of Chinese ecommerce company Alibaba recently said, "The world is going to be about data. Data is going to be so important to human life in the future."

By now, most organizations should be aware of the General Data Protection Regulation (GDPR), and have at least a basic understanding of whether and how it may impact their operations. While we are still in the early days of enforcement, and despite seeing data privacy authorities in Europe operating with a healthy amount of reasonableness, regulators are very serious about ensuring the mandates of the law are carried out across companies of all sizes and industries. Further, jurisdictions around the world, including Australia, Brazil, Japan, and South Korea, are enacting or revising their own data protection regulations. In the United States, while the federal government continues to remain static on implementing federal data privacy legislation, states are taking action.

For example, California passed the California Consumer Privacy Act, Washington state considered the Washington Privacy Act with substantial support, and debates are ongoing in New York and other states for the development of similar legislation. Legal counsel must watch these developments closely and gain a deep understanding of how new and emerging laws, down to the local level, will impact their clients' digital risk profile. The responsibility of getting involved with legislators at the state and federal level to guide the breadth of any new laws and how they will affect businesses also falls on business leaders and their legal teams.

Below, we'll discuss how privacy issues can arise in the context of digitalization implementation.

Digital transformation in action

Most digitalization projects are aimed at reducing cost, streamlining manual processes, and optimizing business functions. Attaining these benefits, however, introduces some key challenges. According to Gartner, these include:

- **Changing sources of corporate value:** Data rights, customer trust, and networks are increasingly valuable assets that need legal safeguards.
- **Faster and less centralized decision making:** This exerts extreme pressure on traditional legal and compliance controls and risk management practices.
- **A reliance on customers' trust and data:** This demands new models of information governance.

Underestimation of these challenges, as well as the legal and compliance ramifications across applicable privacy legislation and data protection and breach notification requirements, can result in serious consequences.

For example, bring your own device (BYOD) initiatives draw some parallels to how these issues can take shape. Not long ago, a business shift to BYOD was the center of countless struggles between corporate legal and IT departments. IT implemented projects focusing exclusively on managing roll-outs as quickly as possible. Before long, counsel realized the many risks that come into play with a new BYOD environment, including the use of third-party applications that generate large amounts of data completely outside the enterprise-controlled IT environment. Thus, battles ensued with legal departments seen as an impediment to execution, rather than a partner in moving the project along the right way. Today, the BYOD disagreement dust has settled at most organizations and, in hindsight, it serves as a solid example of the importance of bringing the company general counsel into the early stages of decision-making and planning for new IT implementations.

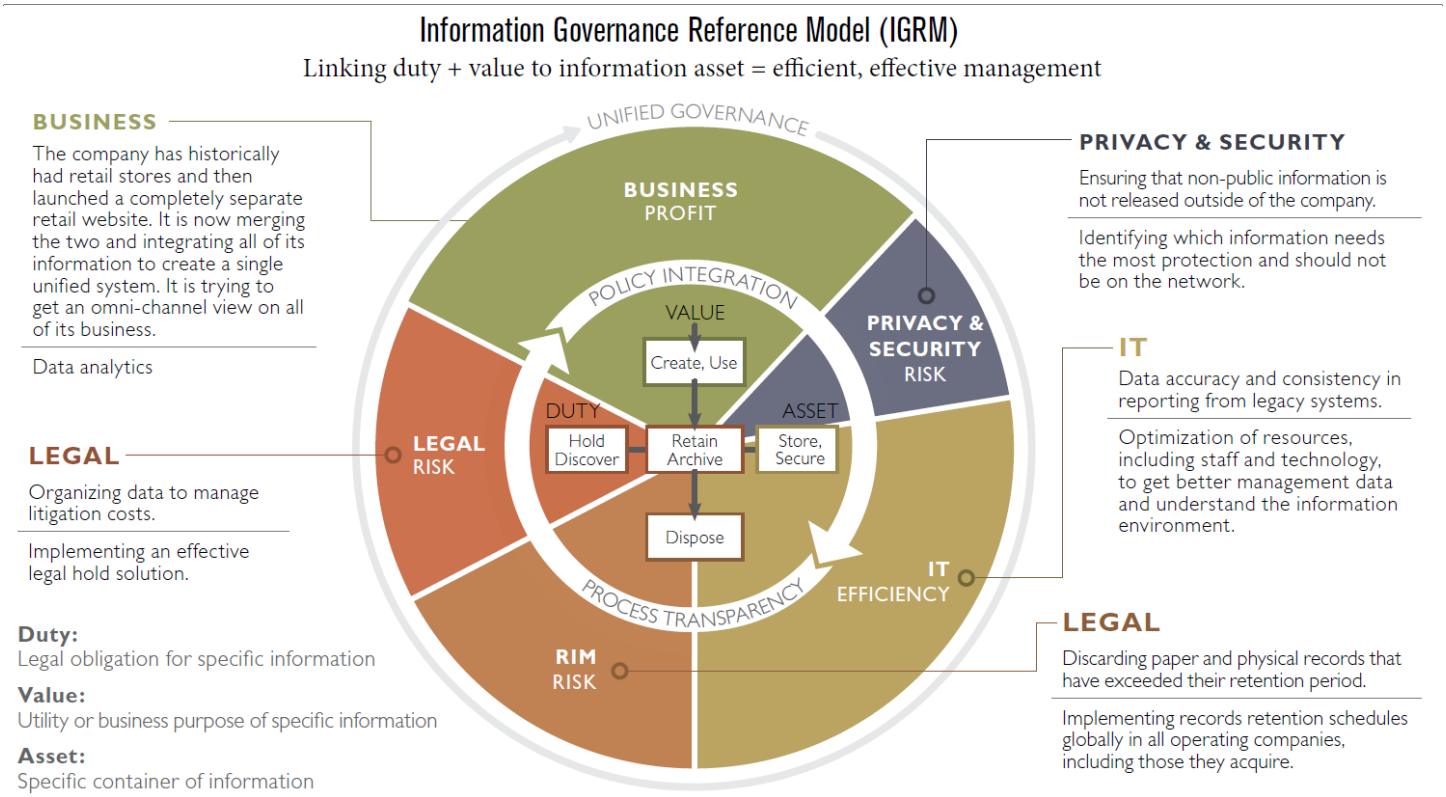
Contractual obligations pose additional issues. Many contracts require approval for data movements and requirements to delete data once the contract terms have been met or expire. For example, personally identifiable information, such as physical addresses and even Social Security numbers, is often collected in conjunction with the performance of contracts, particularly among companies working with individual contractors or private partners. Organizations are required to protect the privacy of such information in the same way that they protect consumer data and ensure that it is not inappropriately shared or breached. Without sound legal process around these activities, and automation in place to ensure that obligations are carried consistently and reliably, it becomes very difficult to maintain contractual compliance and allow digitalization impacting those requirements to move forward.

What is digitalization?

Before in-house counsel can effectively tackle these issues, they must begin with a clear understanding of what digitalization is, and what it means in relation to their responsibilities. Gartner, in its IT Glossary, defines digitalization as "the use of digital technologies to change a business model and provide new revenue and value-producing opportunities … [and] the process of moving to a digital business."

Based on this definition, "digitalization" is distinguished from "digitization," which most agree is the procedure of taking analog content and converting it to digital information capable of being electronically stored, shared, and — most important to digitalization — analyzed in conjunction with improving business process. A Brookings report in 2017 notes astutely that digital technology "has emerged as arguably the most important driving force in the economy today," leading organizations head-first into projects intended to streamline commerce, supply chains, and individual stakeholder and user interaction. In-house counsel are often not involved in decision-making around these types of IT-driven projects and are left scrambling to address the related legal and compliance risks after an implementation is already underway.

Office365 and other cloud migrations are additional examples of major digitalization projects fraught with potential legal peril since the efficient exchange and movement of data is integral to the operation and effectiveness of cloud-based tools. Many organizations are currently working on completing enterprise migrations to these tools and are stalled by unexpected legal and compliance obstacles. In the context of realizing digitalization goals, organizational leadership must carefully consider: where servers and storage infrastructure are physically located, where data users are based, and how data is moved across borders, in advance of determining data storage location to ensure effective access and use to data as well as legal compliance. Jurisdictional privacy regulation increasingly determines the freedom or restriction on data movement and failure to strictly comply with data subject consent and notice requirements is fertile ground for project frustration. Without advance planning and development of compliance processes related to data storage and movement, the legal department then becomes a barrier, rather than an asset, to digital transformation.



Do not forget that, in each potential case, data privacy subject rights raise additional considerations. The GDPR's "right to be forgotten" and the right to prohibit the sale of personal data require legal forethought in digitalization projects. These rights provide individuals with explicit access to their personal data, and the ability to order its erasure. Organizations must respond to requests within one month, leaving little time to perform a potentially large data discovery task. To do this, response teams must be able to quickly find personal data across the enterprise from all sources including the cloud, email, audio files, backups, hard copies, and other data stores. Operationalizing data subject rights is difficult enough on its own without the element of new and unknown data sources borne from digitalization projects. Regulators will not be easy on organizations that fail to adequately fulfill data subject rights. Therefore, legal teams must be looped into digitalization projects that create new and unexpected stores of personal data so they can apply rigorous controls and processes around it.

Data privacy regulations also require that companies ensure the data is accurate and only keep information for as long needed based on the purpose for which it was collected. This hits on another key issue: data quality and retention. When digitalization projects start, companies soon discover that some of the data is stagnant or useless, which dilutes its overall quality and value. It can also raise legal concerns. In an effort to improve data quality, counsel must provide oversight and guidance of data retention laws and legal hold requirements so they can be baked into digitalization projects from the start.

Lawyers are reluctant tech users

In a recent survey, Bloomberg Law reported that lawyers are lacking in their adoption of AI tools. Slow adoption of AI for legal functions (such as eDiscovery and defensible data disposal) underscores the persistent challenge of bridging lawyers and technology. While the survey focused on AI within the legal practice, it did identify that one of the most common reasons for lagging adoption is lack of time and mindshare to learn new tools. Interestingly, law firm respondents in the survey named lack of tech savvy as the top reason why they are not embracing advanced tools at a

faster rate.

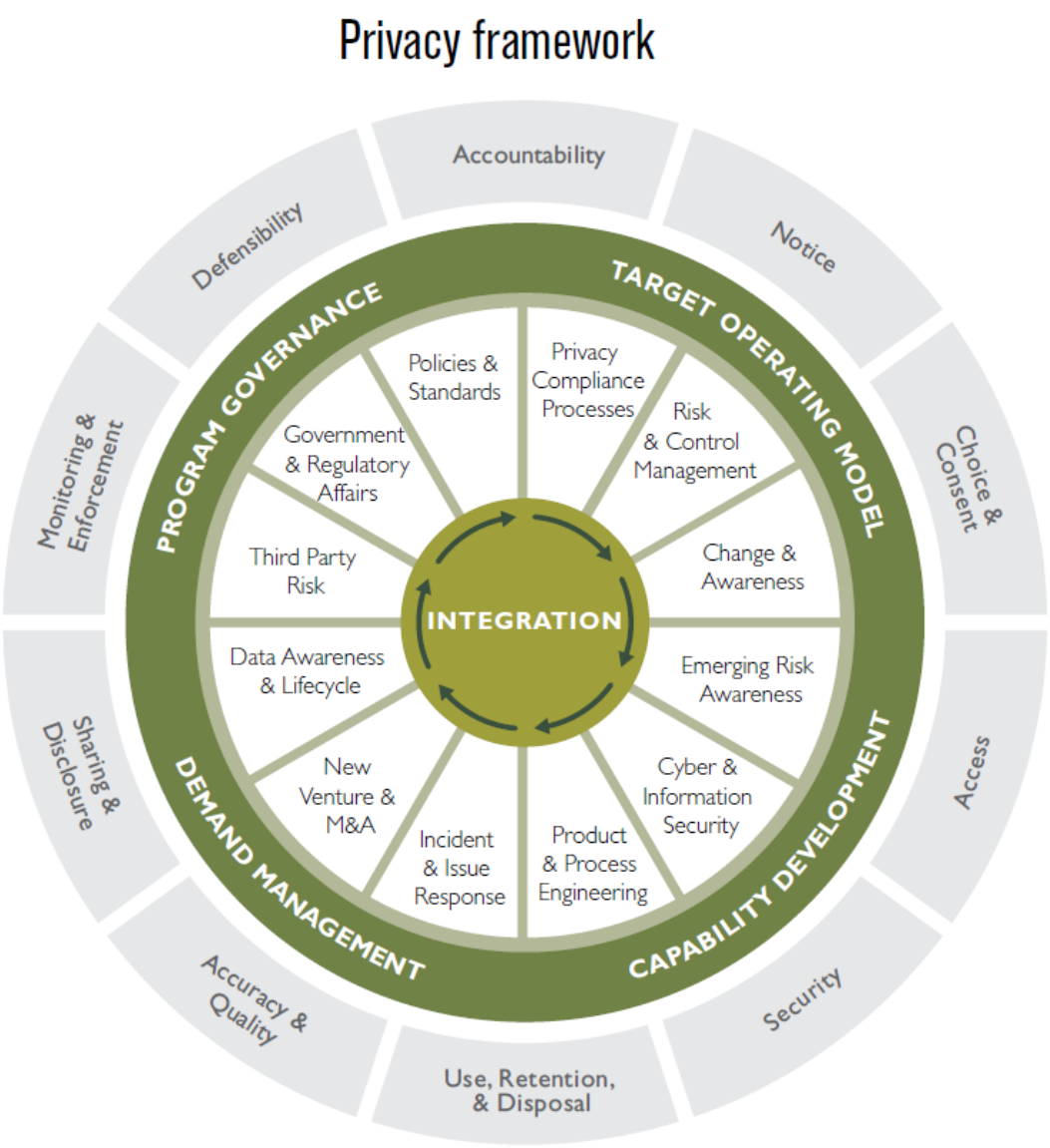
So, in addition to lagging in embracing and enabling digitalization as a whole, lawyers are also not leveraging digitalization in their own practice. As a result, they are unable to fully understand the usefulness and benefits of digitalization.

Conversely, counsel who prioritize both an understanding of technology and an engaged use of it within their own functions will be in a stronger position to partner (rather than impede) in digitalization projects within other areas of the organization.

Counsel as an ally, not a barrier

The legal department has a significant opportunity to help enable change and serve as a support system to move important digitalization projects forward. They can do so in a way that gets ahead of anticipated risks by addressing the following areas:

- **Education:** Corporate education is critical. An attuned and effective GC understands the matrix of risks that come from digital projects at the outset. Thus, lawyers must be open to education about new and novel technology. At the same time, digital project implementation teams must be willing to understand the importance of addressing the sometimes cumbersome legal impacts of the project. This shared respect across practice groups will ensure legal is plugged into projects proactively, rather than reactively, and help avoid unnecessary impediments.
- **Strategic information governance:** In addition to education, a data risk assessment is a solid initial step in understanding the full breadth of risks that apply to the organization and the data it stores. The results of the assessment allow counsel to map data sources and storage locations so legal has a clear picture of exactly where sensitive data lives and what, if any, controls are already in place around it. With this information, legal can work closely with other internal stakeholders to ensure legal compliance and establish policies and workflows that address retention and defensible deletion, access controls, documentation of programs, incident response, etc.
- **Establish risk tolerance:** Counsel must work with executive leadership and the board of directors to define the organization’s stance on risk tolerance. Where the company falls on the spectrum between high- and low-risk tolerance will provide an important guide for the depth and stringency of IG programs and governance over digitalization.



The Sedona Conference provides useful guidance on how organizations can evaluate risk tolerance and conduct a cost/benefit versus risk analysis of information governance programs. According to Sedona, there are cost benefits to robust IG including fewer manual search resources, reduced storage, retrieval and handling of paper records, and lower IT overhead for managing data infrastructure. Further, Sedona notes that information governance can reduce organizational risk exposure by reducing retention of duplicate and ephemeral records, mitigating potential reputational damage, improving compliance with legal recordkeeping requirements, and enhancing protection of the organization's and third parties' confidential, sensitive, and private information. These factors can be weighed against each other to help counsel establish a balance that makes sense for the organization's unique circumstances.

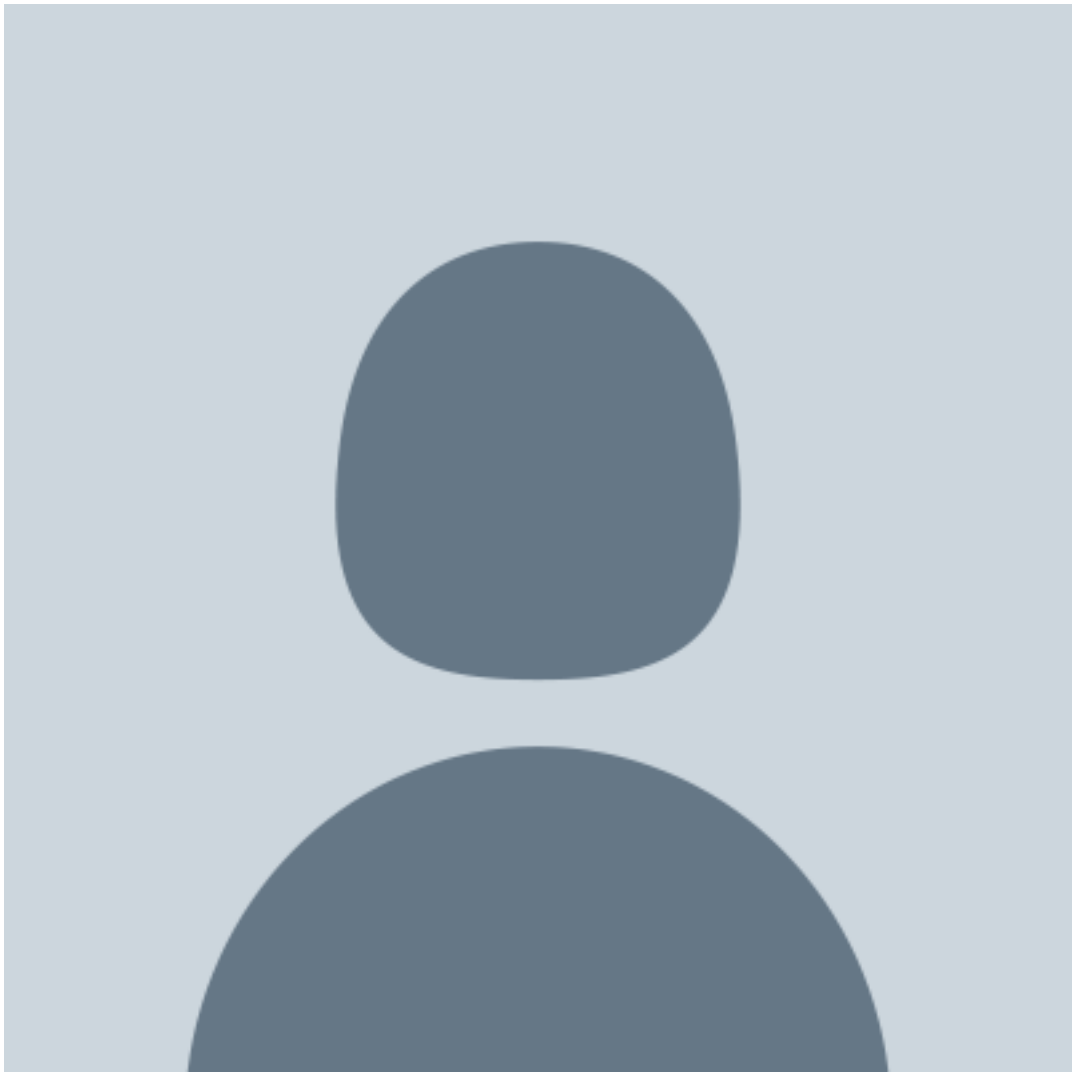
- **Rapid response capabilities and going to scale:** While a digital business' needs may change quickly, and each organization is different, many teams face the same obstacles time and again. In general, digitalization requires "the organization to deal better with change overall, essentially making change a core competency." The GC must understand and be prepared to address common obstacles. These may include aligning business operations with risk tolerance, change management, staff education, and training. As a best practice, internal legal leadership should prepare for these challenges so they can move quickly when new digitization initiatives arise. Gartner advises that the legal team implement workflows to standardize its response to new IT projects and "build a department capable of service model

change and innovation.”

Setting a new pace

In the report mentioned earlier, Gartner found that the legal organizations keeping pace with digitalization delivered “three-and-a-half times fewer projects with inappropriate risk taking and two-and-a-half times fewer delayed projects.” These are impressive metrics, and legal teams achieving them are establishing themselves as business drivers and strategic enterprise partners instead of roadblocks to change. Getting to this standard, however, requires dedicated work by counsel, IT leaders, and other corporate stakeholders. Most importantly, legal and IT should aim to build bridges between their functions, and establish a common understanding of the legal and compliance risks and data sensitivities that arise with new technology deployments. With proactive collaboration in decision-making around the types of data IT deployments are generating and how they are managed, legal can reverse the current dynamic and set a new pace for digital transformation initiatives.

Blaise Benoit



Senior Attorney

SemGroup Corporation

Blaise Benoit is a senior attorney at SemGroup Corporation, a North American operator of pipeline, refinery-connected storage, and deep-water marine terminal infrastructure. He spent much of his career practicing in Southeast Asia and currently advises the executive management of SemGroup’s US Gulf Coast assets.

Deana Uhl

Senior Director

FTI Technology

Deana Uhl is a senior director in the FTI Technology practice and is based in Houston, TX. Uhl provides consulting to corporate clients, with a focus on designing, implementing, and enabling change management for information governance, data privacy, data security, and eDiscovery.