Submitted as part of the proceedings of the December 1, 2018 Capstone Legal Conference on E-Discovery
National Law School of India University, Bangalore

Picking up the Slack™

Legal and Information Governance Considerations for New(er) Technologies

James A. Sherer•
Partner, Chair Information Governance Team
Baker & Hostetler LLP
New York, NY, USA
jsherer@bakerlaw.com

Aaron Singer
General Counsel and SVP of People & Administration
Boxed
New York, NY, USA
aaron@boxed.com

S. Benjamin Barnes
Staff Attorney
Information Governance Team
Baker & Hostetler LLP
Cleveland, OH, USA
bbarnes@bakerlaw.com

By their nature, disruptive technologies change the way we work. But contrary to popular opinion, organizations that ignore these technologies do *not* miss out on the potential benefits they may bring, because this is an age when employees will embrace these technologies if they help get the job done, regardless of institutional permission or approval.[1] Even acknowledging this still raises a host of new challenges, such as how to wrangle these technologies into existing specifications, or how to deal with exceptions.

If the decision to officially adopt a technology isn't difficult enough, another challenge arises when employees start communicating or utilizing a new platform: how to treat the information those applications create, maintain, or store. Generally, an organization's information is categorized as a "record" or as "disposable information." A "record" in this context is what it sounds like: information that an organization should maintain because it has enduring business value or because it must be kept for legal, regulatory, accounting, or audit purposes. Information *outside* this definition is then disposable information, and generally may be discarded after it has served its purpose (again, absent any pending legal hold). When technologies aren't designed to save information (such as Voice over IP phone systems),[2] requirements to manage generated data are restricted for the most part *to* regulatory requirements that serve to create exceptions.[3] And when technologies are designed to avoid retention,[4] they seem to (currently) avoid retention responsibilities generally unless they also meet strict regulatory requirements.[5]

The trickier subject is the technology that falls in the middle, where, depending on how an application is used, it might be one or the other. Subsequently, the question as to whether the

---

• The views expressed in this article are solely those of the authors, should not be attributed to their places of employment, colleagues, or clients, and do not constitute solicitation or the provision of legal advice.

[1] Kenneth R. Fleischmann, *Do-it-yourself information technology: Role hybridization and the design–use interface*. Journal of the American Society for Information Science and Technology 57.1 (2006): 87-95.

[2] Clive Longbottom, *Preventing spam over IP telephony*, ComputerWeekly (Jan. 2007). https://www.computerweekly.com/feature/Preventing-spam-over-IP-telephony (last visited Oct. 9, 2018).

[3] Tim Greene, *VoIP and compliance regulations make strange and difficult bedfellows*, Network World (Sep. 13, 2010). https://www.networkworld.com/article/2218300/compliance/voip-and-compliance-regulations-make-strange-and-difficult-bedfellows.html (last visited Oct. 9, 2018).

[4] Neal Ungerleider, *How Whisper Survives As Other Anonymous Social Apps Like Yik Yak Fail*, Fast Company (Jun. 23, 2017) https://www.fastcompany.com/40424834/how-whisper-survives-as-other-anonymous-social-apps-like-yik-yak-fail (last visited Oct. 9, 2018); *see also 6 Self-Destructing Messaging Apps Adults Need to Know*, ICDL Arabia (Apr. 11, 2017) https://onlinesense.org/6-self-destructing-messaging-apps-adults-need-know/ (last visited Oct. 9, 2018).

[5] Laura Palk, *Gone but Not Forgotten: Does (or Should) the Use of Self-Destruction Messaging Applications Trigger Corporate Governance Duties*, Harv. Bus. L. Rev. 7 (2017): 115.

information created is a record or if it is disposable information in turn raises a number of challenges. We address these challenges in this article, but start with this proposition: if an organization is employing a new technology not directly addressed by regulation, it is best positioned to determine whether that technology creates records or disposable information through its use, and can define policies and practices that support that determination.[6]

To make that decision, and to confront related challenges, organizations should make themselves aware of innovative technologies and the affects they may have when creating or modifying an organization's information. While the organization may not ultimately prohibit employees from these tools' uses, they should (and may be required) to determine how information associated with the tools is governed, where it is stored, who has access it, how the organization might protect it, and how to preserve, review, and produce the information when litigation or a regulatory investigation is likely.[7]

Why Slack?

This perspective is universal, but might best be considered using a case study. Fortunately, Slack is a perfect example of a disruptive technology which many organizations are using—but are perhaps not considering as part of their normal IT and legal practices (and through no fault of Slack's). Slack is a cloud-based[8] digital platform aimed explicitly at collaboration.[9] With nothing more than a name and email address, an individual can quickly set-up a shared space and start communicating. Documents may be uploaded, employees may discuss issues in a public forum, messages sent between those in a specific group, and messages sent in private between individuals.

Unlike some more traditional collaborative software (like email or certain versions of SharePoint[10]), this information lives in the cloud and may rest entirely outside the control or awareness of the organization. And unlike certain other platforms, Slack messaging is not directed solely towards ephemeral contact.[11] In fact, Slack can take the place of email communication, with one survey noting that "internal email [was reduced] by 48.6%,"[12] and this may apply to millions of current employees.[13] While that change in communication is itself remarkable, it also means that data that might otherwise be expected to reside within the

[6] While keeping exceptions related to legal hold implications firmly in mind.
[7] The Sedona Conference Working Group on Electronic Document Retention & Production, *The Sedona Conference Commentary on Legal Holds: The Trigger and the Process* (2010).
[8] Amazon Web Services ("AWS"), *Slack Case Study* (undated). https://aws.amazon.com/solutions/case-studies/slack/ (last visited Oct. 9, 2018).
[9] Slack, *Why Slack? How it Works* (undated) at https://slack.com/features (last visited Oct. 9, 2018).
[10] Microsoft, *SharePoint – Your mobile, intelligent intranet* (undated) at https://products.office.com/en-us/sharepoint/collaboration (last visited Oct. 9, 2018). SharePoint is designed to "[s]hare and manage content, knowledge, and applications to empower teamwork, quickly find information, and seamlessly collaborate across the organization." SharePoint is also operable in Microsoft's Office Hybrid Cloud.
[11] Julia Carpenter, *Sarahah is the latest anonymous app under fire*, CNN Tech (Aug. 28, 2017) (discussing, among other applications, Sarahah, Yik Yak, Whisper, and Secret) https://money.cnn.com/2017/08/23/technology/culture/sarahah-anonymous-apps/index.html (last visited Oct. 9, 2018).
[12] Heather A. Johnson, *Slack*. Journal of the Medical Library Association: JMLA 106.1 (2018): 148.
[13] Melanie Ehrenkranz, *What's Slack Doing With Your Data?* Gizmodo (Jan. 10, 2018) https://gizmodo.com/whats-slack-doing-with-your-data-1820838887 (last visited Oct. 9, 2018).

company takes on a different dimension if the organization is required to maintain certain information as records, or if the information is required for electronic discovery and legal holds if litigation or other regulatory matters arise. Below, we address how organizations might prepare to address new and disruptive technologies like Slack while considering important legal and information governance issues. This is focused on a clear approach to new technologies generally, taking definite and affirmative steps to address and mitigate the risks created by the technologies, and creating a plan for implementing and executing on legal holds should litigation, regulatory inquiries, or other preservation obligations arise.

Information Governance and Shadow IT

The first issue to consider when addressing the possibility of new technologies (including Slack) is the growth of "Shadow" or "Credit Card IT." Shadow IT is the infrastructure that builds up within an organization "without explicit organizational approval,"[14] often using personal or division credit cards (rather than the normal procurement process), that implements new technologies without the awareness and support of IT. This may lead to serious risks, as without the support and control of the organization's IT or IS teams, security flaws may open the organization to cyberattacks or data breaches.[15] And without legal team awareness, the implementation of a legal hold or collection for eDiscovery become exponentially difficult, if not impossible. In these cases, even if the organization's lawyer is unaware of relevant information stored on a Shadow IT system or entirely offsite, the organization may still be responsible for that information held by its employees or even independent contractors[16]—and may face sanctions if relevant information is altered, lost, and ultimately not produced.

Implementing New Technologies – *Asking* The Hard Questions

Organizations with good information governance practices can manage risk while still providing access to and use of valuable information and appropriate technologies. This approach should also apply to new technologies like Slack, but the framework should guide the process—not the technology. That framework starts with a series of questions and inquiries aimed at whether the technology is appropriate as presented for the organization, and whether and how the technology can be responsibly integrated. This also may assist an organization deciding whether information created and maintained on these new systems should be treated as records, and therefore maintained in accordance with a record retention schedule; or as disposable information, which should be disposed of in accordance with the information governance policies. These questions are not magic. Instead, they focus on understanding the tool's operation and capabilities with the backdrop of the organization's use, needs, and requirements.

- **How is the tool being used in the organization—and by whom?**
  In this case, is Slack being used by employees? And can the organization determine that

[14] Jacek Materna, *Shadow IT: it's not what you think*, CSO Online (Dec. 5, 2017). https://www.csoonline.com/article/3239849/it-strategy/shadow-it-its-not-what-you-think.html (last visited Oct. 9, 2018).
[15] Travelers, *Shining a light on Shadow IT*, Global Technology's Risk Advisor Series (2017). https://www.travelers.com/iw-documents/business-insurance/tech-shadow-IT-BTCWH.0004.pdf (last visited Oct. 9, 2018)
[16] *See Haskins v. First American Title Insurance*, 2012 WL 5183908 (D.N.J. Oct. 18, 2012).

simply by querying the active IT environment? It may be that employees are using the tool, for work purposes, on a bring-your-own-device or "BYOD" platform, in which case corporate IT may be unaware or even prohibited from determining its use.[17]

- **Is the organization—or anyone within it—paying for the tool?**
  It may be that employees are using a paid version of the Slack tool[18] that offers search functionality or export settings.[19] Payment for the tool also brings with it greater functionality and insight into where the organization's data (and sometimes secrets) reside, as well as providing slightly more comfort regarding the ongoing viability of the tool.

- **Who holds the organization's data?**
  The platform may provide cloud-based, endpoint or device-based, or hybrid approach. As noted above, Slack is primarily a cloud-based tool, and because it has focused on providing "disparate communication tools [in] a single, unified platform," that "puts an increased burden on Slack to ensure that its customers' information is safe."[20]

- **Who has access to the organization's data?**
  This may not be clear, even in paid instances. At least one commentator noted that employees at Slack "might look at your data under certain circumstances, like if you are experiencing an issue with the app."[21] And that access does not end with Slack—because it, in turn, is using AWS services to host the data.[22] Do both Slack and Amazon have access to the organization's data, and what does that access entail?

- **How is the tool being used?**
  Is it more social or are serious business decisions being made on the platform? Can employees upload files to the environment? Can employees communicate on the tool or otherwise generate new content in the environment? In the case of Slack, it provides a messaging platform that can operate both standalone as well as integrating with "and unif[ying] a wide range of communications services, such as Twitter, Dropbox, Google

[17] Melinda L. McLellan, James A. Sherer & Emily R. Fedeles, *Wherever You Go, There You Are (With Your Mobile Device): Privacy Risks and Legal Complexities Associated with International 'Bring Your Own Device' Programs*, 21 Rich. J.L. & Tech 11 (2015).
[18] Slack, *Slack For Teams* (undated) at https://slack.com/pricing (last visited Oct. 9, 2018). Slack offers three models: per-user "Free," "Standard," and "Plus" packages.
[19] Melanie Ehrenkranz, *What's Slack Doing With Your Data?* Gizmodo (Jan. 10, 2018). https://gizmodo.com/whats-slack-doing-with-your-data-1820838887 (last visited Oct. 9, 2018).
[20] Amazon Web Services ("AWS"), *Slack Case Study* (undated). https://aws.amazon.com/solutions/case-studies/slack/ (last visited Oct. 9, 2018).
[21] Melanie Ehrenkranz, *What's Slack Doing With Your Data?* Gizmodo (Jan. 10, 2018). https://gizmodo.com/whats-slack-doing-with-your-data-1820838887 (last visited Oct. 9, 2018).
[22] Amazon Web Services ("AWS"), *Slack Case Study* (undated). https://aws.amazon.com/solutions/case-studies/slack/ (last visited Oct. 9, 2018). (Slack uses "Amazon Simple Storage Service (Amazon S3) for users' file uploads and static assets.").

Docs, Jira, GitHub, MailChimp, Trello, and Stripe."[23] Does Slack maintain those communications, or simply interface with them?

- **What information is stored or created by the tool?**
  Do users upload files from other systems into the tool? Are these (or other) files modified or edited within in the tool? Are user controls consistent with other applications being used to protect uploaded files? What additional information or metadata from other tools or systems is integrated into or stored on the new tool? Slack, through its API,[24] offers easy integration with many other applications. This may allow for information from other applications to be stored in or modified within the new tool, but also means that users may not know when additional information is transferred outside of the organization if it is embedded in other files.

- **Can you export [your] data from the tool—and, if so, how?**
  Some organizations can hold the organization's data "hostage" until additional fees are paid, and/or an account is made current.[25] This is not a "ransomware" type situation, although some of the basic tenets of ransomware *preparedness* might apply.[26] Slack offers an option to export workspace data in two forms: a "Standard Export" available on "any plan," as well as a "Corporate Export" available on the "Plus plan;[27] organizations may consider these options when determining how, if at all, they treat Slack information as corporate records. In addition, certain third-party vendors offer eDiscovery-related services through Slack's API[28] or otherwise provide collection methods[29,30] in those instances the organization is reacting to requests rather than making policy.

Implementing New Technologies – *Answering* The Hard Questions

To answer these questions, organizations must utilize a variety of methods. Most of these involve direct communication with employees or users, but there are some notable and important exceptions to that heuristic. First, the organization should determine a project lead or point-person for the organization's approach to new technologies generally, or (at least) the specific new technology at issue. Once determined, the lead should assemble a team to consider the technology from those perspectives important to the organization. Depending on the

[23] Amazon Web Services ("AWS"), *Slack Case Study* (undated). https://aws.amazon.com/solutions/case-studies/slack/ (last visited Oct. 9, 2018).
[24] Slack, *Build – internal tools* (undated) at https://api.slack.com/ (last visited Oct. 9, 2018).
[25] Michael G. Van Arsdall, *When Dealing With E-Discovery Vendors, Do You Know Where Your Data Is?* Data Law Insights (Jan. 24, 2013).
[26] James A. Sherer, Melinda L. McLellan, Emily R. Fedeles, and Nichole L. Sterling, *Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 Rich. J.L. & Tech. Ann. Survey (2017). ("[I]ndustry best practices for business continuity include maintaining robust backups that would protect against [data held hostage]," which is applicable—when available—for cloud tools).
[27] Slack, *Workspace Administration* (undated). https://get.slack.help/hc/en-us/articles/201658943-Export-your-workspace-data (last visited Oct. 9, 2018).
[28] Slack, *Onna Discovery* (undated). https://slack.com/apps/A8H1FEU8Z-onna-discovery (last visited July 22, 2018).
[29] Casey C. Sullivan, *How to Obtain Slack Data for Discovery and Investigations*, Closing the loop (Apr. 26, 2018). https://blog.logikcull.com/how-to-obtain-slack-data-for-discovery (last visited Oct. 9, 2018).
[30] Joe Pochron, *Need to Collect Data from Slack? Read this First*, A Transperfect World (Mar. 22, 2018). http://www.transperfect.com/blog/need-to-collect-data-from-slack--read-this-first (last visited Oct. 9, 2018).

organization's size, this team might bring together key stakeholders from legal, IT, and information governance, as well as privacy, operations, and HR as needed.

The lead should then use the framework presented above to evaluate the tool, asking the same questions in a variety of different ways. The lead should start with the employees: to determine who is using the tool for business purposes, and how (including the issue of paying for it). The lead should also feel free to reach out to the technology's own representatives, especially in those instances where the tool provides a paid service, to establish a clear line of communication if there is a future issue of significance for the organization that in any way implicates the tool or its use.

Building Consensus

These conversations should determine the value that a tool (like Slack) brings to the enterprise; the types of information that are implicated; and general considerations of how the information is likely handled. These discussions with stakeholders within and without an organization can highlight what the tool will be used for and help define the contours of future controls or limitations. This also helps organizations address whether information generated in or by the application should be retained as a record generally, only under specific circumstances, or never—and certain organizations opt to treat these types of applications as ephemeral only except for extraordinary circumstances. An additional benefit of involving stakeholders early in the process helps employees feel that their business needs are being considered, and helps with future buy-in for those policies where individual compliance is required.[31]

Discussions with stakeholders will help determine capability requirements for the tool, appropriate licenses, and related controls. As discussed above, Slack offers a variety of licenses that provide an organization with different levels of controls and tools for information management,[32] which should allow an organization to determine the correct price and integration point. These considerations also provide for more specific management associated with the organization's data, which then will incorporate the organization's existing policies on eDiscovery, retention, security, and compliance. In addition, and as mentioned above, Slack has an active API community[33] with a number of other applications that provide for Slack integration,[34] that the organization may want to restrict or block entirely due to the risk of sharing sensitive information.

Policy Considerations

Those considerations associated with information management matter when considering document retention and deletion, as, at least for Slack, the default is permanent retention.[35] As

[31] Tara M. Wood & Cate Kompare, *Participatory Design Methods for Collaboration and Communication.* Code {4} Lib Journal 35 (2017).
[32] Slack, *Slack For Teams* (undated) at https://slack.com/pricing (last visited Oct. 9, 2018).
[33] Slack, *Build – internal tools* (undated) at https://api.slack.com/ (last visited Oct. 9, 2018).
[34] Amazon Web Services ("AWS"), *Slack Case Study* (undated). https://aws.amazon.com/solutions/case-studies/slack/ (last visited Oct. 9, 2018).
[35] Slack, *Workspace Administration - Customize message and file retention policies* (undated) https://get.slack.help/hc/en-us/articles/203457187-Customize-message-and-file-retention-policies (last visited Oct. 9, 2018). ("By default, Slack keeps all your messages and files for the lifetime of your workspace.")

mentioned above, a record is any document or piece of information that has lasting business value or must be retained for legal or regulatory reasons, but when implementing a new policy, organizations must identify what records, if any, are going to be included on the new service. A policy should identify what the official record is if *Slack* maintains the "record" copy and should then determine how such records will be retained for proper periods of time. Likewise, if information is disposable as policy, that should be clearly communicated to users. This may mean putting controls in place to customize Slack defaults. Additionally, in Slack many users may have the ability to delete or edit a variety of posts.[36] If the wrong archive settings are being used, those edited or deleted posts or messages may be lost forever.

Training matters as well. If an organization defines Slack information as disposable information, employees should know the policy, including what conversations should not take place on Slack and what information may not be used there. The organization should provide criteria to help users determine if a specific piece of information should be treated as a record. An organization should indicate to users where and how they can save important decisions. And organizations should provide contact information for their IG function so that IG questions are quickly and accurately addressed by the right people.

Access and Security

Organizations should take an active role, after determining a tool's use, as to user access and security permissions. The organization may have certain information whose access should be limited only to those employees that require access to perform their jobs. Certain (other) information may be sensitive, proprietary, or otherwise valuable enough that access should be restricted as well. Many new technologies may not have the robust user controls that many traditional systems have. And when applications are integrated through the use of APIs, other user controls might be bypassed or compromised.[37] With the number of applications that can interact with Slack, information that may have user controls in the original application may lose these controls when uploaded to Slack. Organizations should take steps to ensure that if sensitive, important, or valuable information is shared on Slack, access is limited only to those requiring it. Organizations may want to consider a data classification policy to clarify how certain information is to be handled, protected, and with whom the information can be shared with, and audit such compliance through the tool.

One method to address these concerns is a comprehensive information governance program. This may include an information governance policy that provides clear expectations regarding information management, and a related record retention schedule indicating how long certain categories of record should be kept as well as what platform maintains the records (as might be the case with a tool like Slack). These policies would provide guidance to users on the handling, storing, and disposal of both records and disposable information. The aforementioned data classification policy can help communicate the treatment of and limits associated with information residing on certain systems. In this case, Slack allows communication by private *or*

[36] Slack, *Delete shared files*, Slack Help Center (undated) at https://get.slack.help/hc/en-us/articles/218159688-Delete-shared-files (last visited Oct. 9, 2018).
[37] Gunnar Peterson, *The Curious Case of API Security*, Axway Whitepaper (2017). https://www.axway.com/sites/default/files/resources/whitepapers/axway_collateral_api_top_11_threats_en.pdf (last visited Oct. 9, 2018).

public channel; these policies should clarify what information or records should be shared in public or company channels, and what should be limited to private or closed groups. Employees utilizing the tool should be trained on what records and information should or should not be shared through various means, and—again, the new tool should be audited for conformance with the policies.

eDiscovery and Spoliation

Organizations must also plan for the worst, whether inaccessible data[38] or that data related to an obligation to preserve and produce.[39] Litigation or a regulatory investigation is *not* inevitable, but when it does happen, organizations are required to consider that data of theirs that may be held by third-parties.[40] The organization's lead, therefore, should consider how to fulfill obligations to preserve and produce relevant information, even when the difficulties associated with preserving or producing information if a hold and production was necessary are not part of the initial sales discussions. Unlike the majority of this discussion, this obligation exists whether the information is considered a record or disposable information. When first considering and subsequently integrating a new tool, the organization should therefore consider how information could be preserved if an obligation to preserve is created. Organizations might even perform a proactive trial run to determine what data exported from the tool looks like; how to search it; and to identify any other difficulties that might arise when preserving, producing, or reviewing the data. In those instances where a tool is inherited, rather than faced prospectively, a balancing test is the approach most organizations take when evaluating how to responsibly manage the information going forward, as well as determining if any information utilized in the tool is a record.

When a legal hold is required, the organization has the obligation to identify possibly relevant information and take steps to preserve the information, even if in the possession of a third-party (such as Slack)[41] or independent contractor.[42] Organizations should determine that hold process when negotiating the commercial services, and also craft a method to inform relevant custodians as to what information must be preserved. If relevant information is not indexed in the tool, searching for relevant information might be difficult or impossible (but perhaps still required). Organizations should therefore also consider metadata, or "data about data."[43] Metadata often contains information about when the document was created, last modified, its history, and often its author. This information may be central to a matter and its preservation should be considered and addressed as part of the legal hold process as mishandled metadata may be altered or lost completely. Finally, as considered above, the organization should pick a standard method for

[38] James A. Sherer, Melinda L. McLellan, Emily R. Fedeles, and Nichole L. Sterling, *Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 Rich. J.L. & Tech. Ann. Survey (2017).
[39] The Sedona Conference Working Group on Electronic Document Retention & Production, *The Sedona Conference Commentary on Legal Holds: The Trigger and the Process* (2010).
[40] *See Brown v. Tellermate Holdings Ltd.*, 2014 U.S. Dist. LEXIS 90123 (S.D. Ohio July 1, 2014) (holding "[d]iscovery did not go smoothly" with associated Salesforce.com data).
[41] *See generally Brown v. Tellermate Holdings Ltd.*, 2014 U.S. Dist. LEXIS 90123 (S.D. Ohio July 1, 2014).
[42] *See generally Haskins v. First American Title Insurance*, 2012 WL 5183908 (D.N.J. Oct. 18, 2012).
[43] Mike Chapple, *Metadata Follows You Everywhere You Go*, Lifewire (Mar. 22, 2018) at https://www.lifewire.com/metadata-definition-and-examples-1019177 (last visited Oct. 9, 2018).

export and review associated with the tool. With Slack, that might be the "Plus" package,[44] or one of the vendors utilizing Slack's API.

Conclusion

New disruptive technologies will not *happen*—they are *happening*. A given tool may be a great opportunity for an organization to change (sometimes for the better) the way it does business, but it will signal a need regardless, whether shining a light on resources employees require or demonstrating that a corporate IT department is understaffed.[45] Implementing a new tool is not without incident, but clear lines of responsibility, consensus building activities, employee interviews (of both the using *and* tool's organizations) can mitigate much of the risk.

Organizations with a defined approach to an active and influential information governance program, a stress-tested legal hold procedure, and an informed IT department can live without fear of these tools, and focus instead on the benefits they can bring. In sum, the organization should follow Polonius and "to thine own self be true"[46]—knowing what tools exist (and should) in the environment as well as its information and methods of dealing with it may be the only way in which an organization can truly "pick up the slack" with third-party tools.

[44] Slack, *Slack For Teams* (undated) at https://slack.com/pricing (last visited Oct. 9, 2018). Slack offers three models: per-user "Free," "Standard," and "Plus" packages.
[45] Steven A. Lowe, *Don't fear shadow IT -- exploit it and prosper*, InfoWorld (Sept. 28, 2015). https://www.infoworld.com/article/2986214/it-management/dont-fear-shadow-it-exploit-it-and-prosper.html (last visited Oct. 9, 2018).
[46] William Shakespeare, *Hamlet*, Act 1, Scene 3, Page 3 (1603).