Richmond Journal of Law & Technology

Volume 25 | Issue 4 Article 2

8-25-2019

Picking Up the Slack™ Legal and Information Governance Considerations For New(ER) Technologies

James A. Sherer
BakerHostetler

Aaron Singer
Boxed

Ben Barnes
Redgrave

PICKING UP THE SLACK™ LEGAL AND INFORMATION GOVERNANCE CONSIDERATIONS FOR NEW(ER) TECHNOLOGIES•

James A. Sherer[*]
Aaron Singer[**]
Ben Barnes[***]

Cite as: James A. Sherer, Aaron Singer & Ben Barnes, *Picking Up the Slack™ Legal and Information Governance Considerations for New(er) Technologies*, 25 RICH. J.L. & TECH., no. 4, 2019.

• This article was originally presented for comment as part of the proceedings of the December 1, 2018 Capstone Legal Conference on E-Discovery at the National Law School of India University, Bangalore.

[+] 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.

[*] James A. Sherer is a partner with BakerHostetler and chairs the Information Governance team. James holds an MBA, his CIPP/US, CIPP/E, CIPM, FIP, and PLS data privacy professional credentials, the CIP and IGP information governance designations, and the CEDS and eDPC eDiscovery specialist credentials. James is U.S. and Global Chambers® Ranked for eDiscovery and serves as a Life Fellow of the American Bar Foundation.

[**] Aaron Singer is Executive Vice President of Corporate Operations and General Counsel of Boxed, a technology and data-driven e-commerce enterprise delivering consumer packaged goods and other products to its B2C and B2B customers and SaaS, RaaS (Retail-as-a-Service), data analytics, marketing, and logistics services to its' partners. Prior to joining Boxed, Aaron was a Senior Associate in the New York office of Latham & Watkins LLP, where he focused his practice on a range of financial and corporate transactions.

[***] Ben Barnes is an attorney at Redgrave. Ben holds CIPP/US and CIPP/E privacy professional credentials, the CIP and IGP information governance designations, and the CEDS eDiscovery specialist credentials.

I. INTRODUCTION

[1] By their nature, disruptive technologies, or those technologies that introduce change and upset the status quo, modify 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, like regulatory record requirements or existing contractual obligations, or how to deal with exceptions to normal business practices.

[2] As if the decision to officially adopt a technology is not difficult enough, another challenge arises when employees start communicating or utilizing a new platform; that is, how to treat the information that those applications create, maintain, or store. Generally, an organization's information is categorized as either a "record" or as "disposable information."[2] A "record" in this context is just 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.[3] Information *outside* this definition is then disposable information, and generally may be discarded after it has served its

[1] *See* Kenneth R. Flelschmann, *Do-It-Yourself Information Technology: Role Hybridization and the Design-Use Interface*, 57 J. AM. SOC'Y INFO. SCI. & TECH. 87, 93–94 (2006), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.690.1839&rep=rep1&type=pdf [https://perma.cc/2SNW-HHBQ].

[2] *See Document Retention Policy*, SECURITAS, https://www.securitas.ie/stand-alone/data-retention/ [https://perma.cc/HWP2-DC3V].

[3] *See generally* Carl Weise, *What is a Business Record?*, AIIM COMMUNITY (Feb. 3, 2011, 11:02 PM), http://community.aiim.org/blogs/carl-weise/2011/02/03/what-is-a-business-record [https://perma.cc/NV5Z-YV2Y] (explaining how AIIM's ERM and ECM certificate courses determine what a business record is).

purpose—again, absent any pending legal hold.[4] When technologies are not designed to save information—such as Voice over IP phone systems[5]—requirements to manage generated data are restricted, mostly *to* those regulatory requirements that serve to create exceptions to normal practices that might otherwise opt not to save every phone call and received message.[6] When technologies are designed to avoid retention,[7] they are generally not subject to retention responsibilities unless they also meet strict regulatory requirements.[8]

[3] The trickier subject is technology that falls in the middle, where, depending on how an application is used, it might create a record or disposable information, and 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 that is not directly regulated,

[4] *See Document Retention Policy*, *supra* note 2.

[5] *See* Clive Longbottom, *Preventing Spam Over IP Telephony*, COMPUTER WKLY. (Jan. 2007), https://www.computerweekly.com/feature/Preventing-spam-over-IP-telephony [https://perma.cc/JL2H-FG5C].

[6] *See* Tim Greene, *VoIP and Compliance Regulations Make Strange and Difficult Bedfellows*, NETWORK WORLD (Sept. 13, 2010, 7:30 AM), https://www.networkworld.com/article/2218300/compliance/voip-and-compliance-regulations-make-strange-and-difficult-bedfellows.html [https://perma.cc/WQ5N-M8RV] (discussing particular regulations that impact VoIP practices).

[7] *See generally* Neal Ungerleider, *How Whisper Survives as Other Anonymous Social Apps Like Yik Yak Fail*, FAST COMPANY (June 23, 2017), https://www.fastcompany.com/40424834/how-whisper-survives-as-other-anonymous-social-apps-like-yik-yak-fail [https://perma.cc/9FQX-ZXYF] (discussing the various methods the Whisper app has used to successfully monetize user-submitted content while simultaneously maintaining user anonymity); *6 Self-Destructing Messaging Apps Adults Need to Know*, ONLINESENSE (Apr. 11, 2017), https://onlinesense.org/6-self-destructing-messaging-apps-adults-need-know/ [https://perma.cc/8LND-E39W] (summarizing the functionality of six popular "self-destructing" messaging apps).

[8] *See* Laura Palk, *Gone But Not Forgotten: Does (or Should) the Use of Self-Destruction Messaging Applications Trigger Corporate Governance Duties*, 7 HARV. BUS. L. REV. 115, 146–47 (2017).

the organization will be best positioned to determine whether that technology creates records or disposable information by first using the technology, and then by defining policies and practices that support that determination.[9]

[4] To make that decision, and to confront related challenges, organizations should educate themselves on the effects of innovative technologies when those technologies create or modify the organization's information. While the organization may not ultimately prohibit employees from using these tools, 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.[10] This perspective is universal, but might best be considered using a case study.

II. WHY SLACK?

[5] Fortunately, Slack is a perfect example of a disruptive technology that many organizations are using. Through no fault of Slack, this technology is perhaps not considered a part of the organization's normal IT and legal practices. Slack is a cloud-based[11] digital platform aimed explicitly at collaboration.[12] With nothing more than a name and email address, an individual can quickly set-up a shared space and start communicating.[13] On Slack, users can upload documents, employees can

[9] *See id.* at 118.

[10] *See* The Sedona Conference, *The Sedona Conference Commentary on Legal Holds: The Trigger & the Process*, THE SEDONA CONFERENCE J. 265, 275 (2010).

[11] *See Slack Case Study*, AMAZON WEB SERVS., https://aws.amazon.com/solutions/case-studies/slack/ [https://perma.cc/7LKX-HGKG].

[12] *See Why Slack? How It Works*, SLACK, https://slack.com/features [https://perma.cc/ZPF3-KDFY].

[13] *See Start with a Workspace*, SLACK, https://slack.com/get-started [https://perma.cc/2VN9-WZCA].

discuss issues in a public forum, messages can be sent among those in a specific group, and messages can be sent privately between individuals.[14]

[6] Unlike some more traditional collaborative software—like email or certain versions of SharePoint[15]—this information lives in the cloud and may rest entirely outside the control or awareness of the organization.[16] Unlike other platforms, Slack messaging is not directed solely towards ephemeral contact.[17] In fact, Slack can take the place of email communication, with one survey noting that "internal email [was reduced] by 48.6%."[18] This may apply to millions of current employees.[19] While that change in communication is itself remarkable, it also means data that might otherwise be expected to reside within the company takes on a different dimension if the organization must maintain certain information

[14] *See A Channel for Every Conversation*, SLACK, https://slack.com/features [https://perma.cc/S2L5-2T4T].

[15] See *SharePoint, Your Mobile, Intelligent Intranet*, MICROSOFT, https://products.office.com/en-us/sharepoint/collaboration [https://perma.cc/7DV3-AUT4]. SharePoint is designed to "[s]hare and manage content, knowledge, and applications to empower teamwork, quickly find information, and seamlessly collaborate across the organization." *Id.* SharePoint is also operable in Microsoft's Office Hybrid Cloud. *See id.*

[16] *See* '*Case Study': Slack Improves its Security by Using Services in the Cloud*, BBVA (Nov. 3, 2016), https://bbvaopen4u.com/en/actualidad/case-study-slack-improves-its-security-using-services-cloud [https://perma.cc/LBX3-NPNR].

[17] *See, e.g.*, Julia Carpenter, *Sarahah is the Latest Anonymous App Under Fire*, CNN BUS. (Aug. 28, 2017, 6:24 PM), https://money.cnn.com/2017/08/23/technology/culture/sarahah-anonymous-apps/index.html [https://perma.cc/HE56-T5GB] (discussing, among other applications, Sarahah, Yik Yak, Whisper, and Secret).

[18] *See* Heather A. Johnson, *Slack*, 106 J. MED. LIBR. ASS'N 148, 148 (2018).

[19] *See generally* Melanie Ehrenkranz, *What's Slack Doing with Your Data?*, GIZMODO (Jan. 10, 2018, 1:11 PM) https://gizmodo.com/whats-slack-doing-with-your-data-1820838887 [https://perma.cc/ZB64-HK83] ("More than six million people use Slack daily, spending on average two hours each day inside the chat app. For many employees, work life is contingent on Slack . . . .").

as records, or if litigation or other regulatory matters arise and the information is needed for electronic discovery and legal holds.[20] Below, we consider how organizations might begin to address new and disruptive technologies like Slack, while considering important legal and information governance issues. The focus is on a clear approach to new technologies: taking definite, affirmative steps to address and mitigate the risks the technologies create, and should litigation, regulatory inquiries, or other preservation obligations arise, crafting a plan for implementing and executing legal holds.

III. INFORMATION GOVERNANCE AND SHADOW IT

[7] The first issue to consider when addressing the possibility of new technologies that may cause disruptions, 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,"[21] often using personal or division credit cards—rather than the normal procurement process—that implements new technologies without the awareness and support of IT departments.[22] This may lead to serious risks because without the support and control of the organization's IT or IS teams, security flaws may open the organization to cyberattacks or data breaches.[23] Also, without the legal team's awareness of Shadow IT, the implementation of a legal hold or collection for eDiscovery becomes exponentially difficult, if not impossible.[24] In these cases, even if the

[20] *See Data Request Policy*, SLACK, https://slack.com/user-data-request-policy [https://perma.cc/PHM5-RFZ7] (effective May 4, 2017).

[21] Jacek Materna, *Shadow IT: It's Not What You Think*, CSO ONLINE (Dec. 5, 2017, 4:00 AM), https://www.csoonline.com/article/3239849/it-strategy/shadow-it-its-not-what-you-think.html [https://perma.cc/7P2G-TFME].

[22] *See id.*

[23] *See Shining a Light on Shadow IT*, TRAVELERS GLOBAL TECH. RISK ADVISOR SERIES 3, 10, 12 (2017), https://www.travelers.com/iw-documents/business-insurance/tech-shadow-IT-BTCWH.0004.pdf [https://perma.cc/55J4-UF9P].

[24] *See* Bob Krantz & Jeff Fehrman, *Emailgate Highlights the Challenges of Shadow IT*,

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[25] and may face sanctions if relevant information is altered, lost, or ultimately not produced.[26]

IV. IMPLEMENTING NEW TECHNOLOGIES – *ASKING* THE HARD QUESTIONS

[8] 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 inquiries aimed at whether the technology is appropriate as presented for the organization, and whether and how the technology can be responsibly integrated. This framework may also assist an organization in 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.

- **Who is using the tool in the organization?**
  In this case, is Slack being used by employees? Can the organization determine that simply by querying the active IT environment? It may be that employees are using the tool, for work

FOCUSED DISCOVERY (May 20, 2015), https://www.mindseyesolutions.com/2015/05/20/emailgate-highlights-the-challenges-of-shadow-it/ [https://perma.cc/5FNN-HYWN].

[25] *See* Haskins v. First Am. Title Ins. Co., No. 10-5044 (RMB/JS), 2012 WL 5183908, at *1–5 (D.N.J. Oct. 18, 2012).

[26] *See id*. at *12–14.

purposes, on a bring-your-own-device or "BYOD" platform. In such a case, corporate IT departments may be unaware of—or possibly even prohibited from—determining the tool's use in the organization.[27]

- **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[28] that offers search functionality or export settings.[29] 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 or what holds the organization's data?** The platform may provide cloud-based data storage, endpoint or device-based data storage, or a hybrid approach.[30] As noted above, Slack is primarily a cloud-based tool,[31] and because it has focused on providing "disparate communication tools [in] a single, unified

[27] *See* 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. L.J. & TECH. no. 2, at ¶ 54 (2015).

[28] *See Find a Plan*, SLACK, https://slack.com/pricing [https://perma.cc/TN9T-M88Z] (presenting three available account models available: per-user "Free," "Standard," and "Plus" packages).

[29] *See Slack for Teams*, SLACK, https://slack.com/pricing [https://perma.cc/TN9T-M88Z] (explaining the various features available for use at different paid levels of the tool).

[30] *See Hybrid Cloud Architectures with AWS*, AMAZON WEB SERVS., https://aws.amazon.com/enterprise/hybrid/ [https://perma.cc/SZB2-JHCG] (detailing the various different data storage approaches).

[31] *See* James Sanders, *Slack: A Cheat Sheet*, TECHREPUBLIC (Nov. 1, 2018, 4:11 AM), https://www.techrepublic.com/article/slack-the-smart-persons-guide/ [https://perma.cc/8VZD-33C5].

platform," there is "an increased burden on Slack to ensure that its customers' information is safe."[32]

- **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."[33] However, that access does not end with Slack because it is also using Amazon Web Service (AWS) services to host the data.[34] 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 tool? Can employees communicate on the tool or otherwise generate new content in the environment? Slack provides a messaging function that can operate either as a standalone platform or as an integrated one by "unif[ying] a wide range of communications services, such as Twitter, Dropbox, Google Docs, Jira, GitHub, MailChimp, Trello, and Stripe."[35] 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 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 are integrated into or stored on the new tool? Slack, through its Application Programming Interface (API), offers easy integration with many other applications.[36] This may allow for information from other applications to be stored in or modified within the new tool, but this also means that users may not know when additional

[32] *Slack Case Study*, *supra* note 11.

information is transferred outside of the organization if it is embedded in other files.[37]

- **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.[38] This is not a "ransomware" type situation, although some of the basic tenets of ransomware *preparedness* might apply.[39] 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."[40] Organizations may consider these options when determining how, if at all, they treat Slack information as corporate records. In addition, certain third-party

[33] Ehrenkranz, *supra* note 19.

[34] *See Slack Case Study*, *supra* note 11. (indicating that Slack uses "Amazon Simple Storage Service (Amazon S3) for users' file uploads and static assets . . . .").

[35] *Id.*

[36] *See id.*

[37] *See id.*

[38] *See* Michael G. Van Arsdall, *When Dealing With E-Discovery Vendors, Do You Know Where Your Data Is?*, DATA LAW INSIGHTS (Jan. 24, 2013), https://www.crowelldatalaw.com/2013/01/when-dealing-with-e-discovery-vendors-do-you-know-where-your-data-is/.

[39] *See* James A. Sherer et al., *Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 RICH. J.L. & TECH. no. 3, at ¶ 51 (2017) (explaining that "industry best practices for business continuity include maintaining robust backups that would protect against [data held hostage]," which is applicable—when available—for cloud tools).

[40] *Workspace Administration*, SLACK, https://get.slack.help/hc/en-us/articles/201658943-Export-your-workspace-data [https://perma.cc/HB84-U5SN].

vendors offer eDiscovery-related services through Slack's API[41] or otherwise provide collection methods.[42] In those instances, the organization is reacting to requests rather than making policy.

V. IMPLEMENTING NEW TECHNOLOGIES – *ANSWERING* THE HARD QUESTIONS

[9] To answer these questions, organizations must utilize a variety of methods. Most of these involve direct communication with employees or users,[43] 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, or at least the 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 organization's size, this team might bring together key stakeholders from legal, IT, and information governance, as well as privacy, operations, and HR if needed.

[10] 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 inquiring 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

[41] *See Onna Discovery*, SLACK, https://slack.com/apps/A8H1FEU8Z-onna-discovery [https://perma.cc/NC95-DJPZ].

[42] *See* Casey C. Sullivan, *How to Obtain Slack Data for Discovery and Investigations*, LOGIKCULL (Apr. 26, 2018), https://blog.logikcull.com/how-to-obtain-slack-data-for-discovery [https://perma.cc/6MTQ-FR59]; *see also* Joe Pochron, *Need to Collect Data from Slack? Read this First*, TRANSPERFECT (Mar. 22, 2018), http://www.transperfect.com/blog/need-to-collect-data-from-slack--read-this-first [https://perma.cc/M8U7-Q78N].

[43] *See* David Wither, *How to Get Employees on Board with New Technology*, TECH.CO (Nov. 22, 2017, 8:30 AM), https://tech.co/news/get-employees-on-board-new-technology-2017-11 [https://perma.cc/HTQ8-3XUE].

tool provides a paid service, to establish a clear line of communication if there is a future issue of significance that implicates the tool or its use.

A. Building Consensus

[11] 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 outside of 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 the status of the information generated in or by the application, and whether the information should be retained as a record, never, or only under specific circumstances. Certain organizations opt to treat these types of applications as ephemeral only except for extraordinary circumstances.[44] An additional benefit of involving stakeholders early in the process is that it helps employees feel that their business needs are being considered, and it helps with future buy-in for those policies where individual compliance is required.[45]

[12] Discussions with stakeholders will help determine capability requirements for the tool, appropriate licenses, and related controls.[46] As discussed above, Slack offers a variety of licenses that provide an organization with different levels of controls and tools for information management,[47] which should allow an organization to determine the

[44] *See* Adam Henshall, *How to Use Slack Like a Pro and Become a Power User (22 Tips & Tricks)*, PROCESS STREET (Apr. 2, 2018), https://www.process.st/how-to-use-slack/ [https://perma.cc/FW5J-4B28].

[45] *See* Tara M. Wood & Cate Kompare, *Participatory Design Methods for Collaboration and Communication*, CODE{4}LIB J. (Jan. 30, 2017), https://journal.code4lib.org/articles/12127 [https://perma.cc/K7ZF-3GAB].

[46] *See id.*

[47] *See generally Slack for Teams*, *supra* note 29 (outlining the differing Slack subscriptions available).

correct price and integration point.[48] These considerations also provide for more specific management associated with the organization's data, which will then incorporate the organization's existing policies on eDiscovery, retention, security, and compliance.[49] In addition, Slack has an active API community[50] with a number of other applications that provide for Slack integration[51] that the organization may want to restrict or block entirely due to the risk of sharing sensitive information.

B. Policy Considerations

[13] The considerations associated with information management are important when considering document retention and deletion, as, at least for Slack, the default is permanent retention.[52] As 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.[53] A policy should identify what the official record is if Slack maintains the "record" copy and should determine how such records will be retained for proper periods of time. Likewise, if information is disposable as a matter of policy, that should be clearly communicated to users. This may mean putting controls

[48] *See generally id.* (listing features available for each subscription).

[49] *See id.*

[50] *See Slack API: Build*, SLACK, https://api.slack.com/ [https://perma.cc/82ED-8MAS].

[51] *See Slack Case Study*, *supra* note 11.

[52] *See Customize Message and File Retention Updates*, SLACK, http://get.slack.help/hc/en-us/articles/203457187-Customize-message-and-file-retention-policies [https://perma.cc/5LAP-THCC] ("By default, Slack keeps all your messages and files for the lifetime of your workspace.").

[53] *See* Rae Cogar & R. Thomas Howell, *Retention: More Important than Ever*, 13 ABA BUS. L. SEC. 1 (2003), http://apps.americanbar.org/buslaw/blt/2003-09-10/cogar.html [https://perma.cc/M6BA-PUMZ]; *see also* Weise, *supra* note 3.

in place to customize Slack defaults.[54] Additionally, many Slack users may have the ability to delete or edit a variety of posts.[55] If the wrong archive settings are being used, those edited or deleted posts or messages may become lost forever.[56]

[14] 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 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 made on behalf of the organization, or by which the organization is obligated. Also, organizations should provide contact information for their information governance function so that information governance questions are quickly and accurately addressed by the right people.

C. Access and Security

[15] Organizations should take an active role, after determining how a tool is being used, in user access and security permissions. The organization may have certain information to which access should be limited to only those employees that require access to perform their jobs. Certain 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,

---

[54] *Cf.* Herb Weisbaum, *Employers Can Read 'Private' DMs Without Telling Workers*, NBC NEWS (Apr. 5, 2018, 5:42 AM), https://www.nbcnews.com/better/business/slack-updates-privacy-policy-employers-can-read-private-dms-without-ncna862811 [https://perma.cc/KGA7-VU28] (explaining Slack's updated privacy policies and how they are being used to retain employee information without employee's knowledge).

[55] *See Delete Files from Slack*, SLACK HELP CTR., https://get.slack.help/hc/en-us/articles/218159688-Delete-shared-files [https://perma.cc/F4KU-Y5GV].

[56] *See Edit or Delete Messages*, SLACK HELP CTR., https://get.slack.help/hc/en-us/articles/202395258-Edit-or-delete-messages [https://perma.cc/Z5P3-FJ6H].

potentially limiting their functionality or available controls. Additionally, when applications are integrated through the use of APIs, other user controls might be bypassed or compromised.[57] With the number of applications that can interact with Slack, information that may have user controls in the original application may lose those controls when uploaded to Slack.[58] 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—for example, assigning *secret* or *restricted* access to certain data types—to clarify how certain information is to be handled and protected, with whom the information can be shared, and how to audit such compliance through the tool.

[16] One method that an organization may employ to address these concerns is a comprehensive information governance program. This may include an information governance policy that provides (1) clear expectations regarding information management, (2) a related record retention schedule indicating how long certain categories of record should be kept, and (3) what platform maintains the records—as might be the case if an organization is using a tool like Slack. These policies would provide guidance to users on the handling, storing, and disposing of both records and 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* public channel.[59] These policies should

[57] *See generally* Gunnar Peterson, *The Curious Case of API Security: Solving the Top 11 API Threats*, AXWAY (2017), https://www.axway.com/sites/default/files/resources/whitepapers/axway_collateral_api_top_11_threats_en.pdf [https://perma.cc/6Q9V-UJ7E] (discussing the most common vulnerabilities and security risks associated with the use of API).

[58] *See generally id.* (highlighting how app integration through API can cause unanticipated loss of user controls).

[59] *See Create a Channel*, SLACK HELP CTR. (Feb. 21, 2019, 11:07 PM), https://get.slack.help/hc/en-us/articles/201402297-Create-a-channel [https://perma.cc/Z2SG-KCG5].

clarify what information or records should be shared in public or company-wide channels and what should be limited to private or closed groups. Employees utilizing the tool should be trained on what records and information can or cannot be shared through various means, and the new tool should be audited for conformance with the policies.

D. eDiscovery and Spoliation

[17] Organizations must also plan for the worst, whether data is inaccessible[60] or is related to an obligation to preserve and produce.[61] Litigation or a regulatory investigation is *not* inevitable, but when it does happen, organizations are required to consider any data that may be held by third-parties.[62] The organization's lead, therefore, should consider how to fulfill obligations to preserve and produce relevant information if a hold and production become necessary, even when the difficulties associated with preserving or producing information were not part of the initial sales discussion. Unlike the majority of this discussion, this obligation exists whether the information is considered a record or disposable information.[63] When first considering and subsequently integrating a new tool, the organization should 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

[60] *See, e.g.*, Sherer et al., *supra* note 39, at ¶ 1 (discussing Ransomware's ability to encrypt data on devices, causing owners to not have the access to their data).

[61] *See generally* The Sedona Conference, *supra* note 10 (describing a duty to preserve relevant and discoverable information when litigation is reasonably anticipated).

[62] *See generally* Brown v. Tellermate Holdings Ltd., No. 2:11-cv-1122, 2014 U.S. Dist. LEXIS 90123, at *2–3 (S.D. Ohio July 1, 2014) (holding "[d]iscovery did not go smoothly" and finding that Tellermate should have disclosed associated data from Salesforce.com, a third-party).

[63] *See generally* FED. R. CIV. P. 26(b)(1) (explaining the broad scope of discovery in nonprivileged matters).

where a tool is inherited rather than faced prospectively, a balancing test between supporting existing business operations and confronting general policy considerations—as well as other factors—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.[64]

[18] 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[65] or an independent contractor.[66] In addition to organizations determining that hold process when negotiating the commercial services, they should also craft a method to inform relevant custodians regarding 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.[67] Therefore, organizations should also consider metadata, or "data about data."[68] Metadata often contains information about when the document was created or last modified, and its history and 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

[64] *See* Lauren Hilinski, *Comparing Records Management Options: Balancing Cost, Security, and Efficiency*, RECORD NATIONS (Oct. 29, 2018) https://www.recordnations.com/2018/10/comparing-records-management-options-cost-security-efficiency/ [https://perma.cc/U8Q7-M53T].

[65] *See Brown*, 2014 U.S. Dist. LEXIS 90123 at *54.

[66] *See* Haskins v. First Am. Title Ins. Co., No. 10-5044 (RMB/JS), 2012 WL 5183908, at *1, *5 (D.N.J. Oct. 18, 2012).

[67] *See* Jennifer Lonoff Schiff, *14 Things You Need to Know About Data Storage* Management, CIO (Sept. 11, 2013, 8:00 AM), https://www.cio.com/article/2382585/virtualization/14-things-you-need-to-know-about-data-storage-management.html [https://perma.cc/5Y23-MPVQ].

[68] Mike Chapple, *What is Metadata?*, LIFEWIRE (Oct. 4, 2018), https://www.lifewire.com/metadata-definition-and-examples-1019177 [https://perma.cc/G7HP-36U7].

mishandled metadata may be altered or lost completely. Finally, as considered above, the organization should pick a standard method for export and review associated with the tool. With Slack, that might be purchasing or subscribing to the "Plus" package,[69] or engaging one of the vendors utilizing Slack's API.[70]

VI. CONCLUSION

[19] 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.[71] Implementing a new tool is not without incident, but clear lines of responsibility, consensus-building activities, and employee interviews—of both the using *and* such tool's organizations—can mitigate much of the risk.

[20] 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, organizations should follow Polonius and "to thine own self be true,"[72] by knowing what tools should and do exist in the environment, as well as such tools' operation, how the organization's information functions within each tool, and sound methods

[69] *See All Business. All the Time.*, SLACK, https://slack.com/pricing/plus [https://perma.cc/5Z9H-KKTC]. Slack offers three models: per-user "Free," "Standard," and "Plus" packages.

[70] *See* Michelle Burbick, *Slack Beefs Up Developer Tools*, NOJITTER (Feb. 13, 2019), https://www.nojitter.com/team-collaboration-tools-workspaces/slack-beefs-developer-tools [https://perma.cc/F96V-DB3J].

[71] *See* 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 [https://perma.cc/P995-EHGR].

[72] WILLIAM SHAKESPEARE, THE TRAGEDY OF HAMLET, PRINCE OF DENMARK act 1, sc. 3.

of dealing with it. This may be the only way in which an organization can truly "pick up the slack" with third-party tools.