VERITAS | eDJGroup

Legal Considerations of Microsoft Office 365™

Who should read this paper

Information technology practitioners and eDiscovery counsel from organizations that are considering, evaluating, or implementing Office 365.

Veritas™ and Microsoft Office 365™ for eDiscovery and compliance

Legal Considerations of Microsoft Office 365™

Veritas™ and Microsoft Office 365™ for eDiscovery and compliance

Content

Background

eDJ Group profile: Greg Buckles is a highly successful and well-respected independent eDiscovery consultant specializing in eDiscovery for over 25 years. Greg's career spans law enforcement, legal service provider, corporate legal, law firm, and legal software development. This deep and diverse background combines with exposure to the discovery challenges of Fortune 500 clients to provide a unique industry perspective. He has contributed to Sedona Conference and EDRM Working Group publications. He has been a guest speaker and panelist at numerous discovery conferences, webinars, forums, and other public venues, including LegalTech. He has published research papers on many different aspects of electronic discovery, enterprise search, and corporate defensibility.

Research overview: Greg's extensive research and strategic consulting engagements have produced a unique solution perspective of how the Microsoft Office 365™ and Veritas™ products can form a 'better together' solution to meet eDiscovery and compliance requirements. This paper outlines Office 365 trends, functionality, potential challenges, and how his clients are using Veritas products in real world implementations.

Scope limits: Greg is a technical and process expert rather than an attorney. All legal decisions should be made in consultation with counsel. Every organization has unique challenges and requirements that may differ from the trends and best practices relayed in this paper. Finally, all functionality limitations and other technical features described in this paper are based on best available public information and published documentation of the last available product versions and internal research and analysis. Readers should check for new patches, versions, or products before making critical decisions.

What is Office 365 and why does legal care?

In 2011, Microsoft launched Office 365, a set of communications and collaboration software and cloud services offered in a large number of subscription plans. Business and enterprise plans for Office 365 include access to Microsoft® Exchange Online, Microsoft SharePoint® Online, and Microsoft Lync® Online, plus Microsoft® Office Online, and desktop applications like Microsoft® Word, Microsoft® Excel, and more. It is easy to see why many organizations are considering migrating from traditional on-premises solutions to the Office 365 cloud infrastructure.

The migration of core data assets to a cloud platform brings a completely new set of compliance and eDiscovery challenges, especially in the face of escalating regulatory requests. With Microsoft hosting your email and files in the Azure cloud, how can your legal team meet their key preservation and discovery obligations?

Introducing the eDiscovery Center

In October 2012, Microsoft introduced a new eDiscovery Center in Office 365 that serves as a portal for managing legal, regulatory, and investigative matters. It is designed to be straightforward to use and easily accessible to designated discovery managers such as a legal, compliance, and HR professionals.

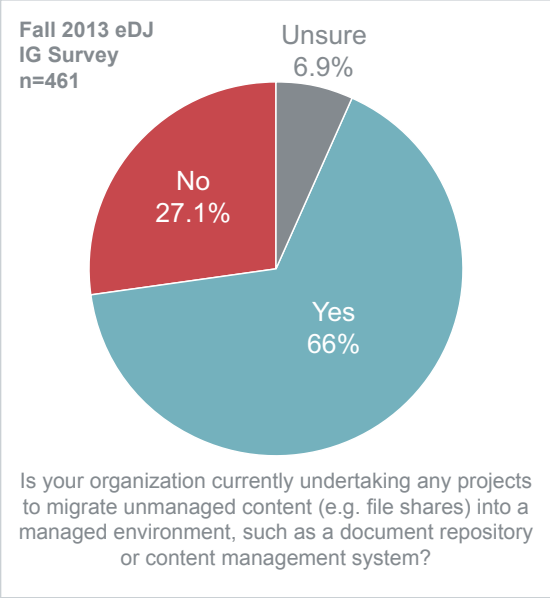
The eDiscovery Center, only available in the more expensive Office 365 E3 and E4 subscription plans, is not a purpose-built eDiscovery platform. It is just a site collection template in SharePoint Online. From the eDiscovery Center site collection template, the discovery manager can create a new case (which creates a new sub-site) from where they can

search across Exchange mailboxes and SharePoint sites, place content on legal hold (In-Place Hold), preview individual search results, and export data to a format that can be consumed by other third-party review and analysis applications.

Microsoft appears to have constructed the workflow, functionality, and features around a relatively specific eDiscovery use-case that presumes limited overlap between matters, no global preservation or search requirements, and no need for in-house Early Case Assessment (ECA), review, and culling by legal teams.

Although it is possible to expand and adapt the eDiscovery Center site collection template to better meet your workflow requirements, you should consider the long-term impact and burden of custom versions running on infrastructure that may not be in your complete control.

How soon do legal teams need to worry about Office 365?



Is your organization currently undertaking any projects to migrate unmanaged content (e.g. file shares) into a managed environment, such as a document repository or content management system?

According to surveys, conference audiences, and active eDJ consulting inquiries, the majority of IT departments are evaluating a migration, running an active pilot user group, or have already begun moving users to Office 365. The result is that the penetration of the Office 365 is expected to more than double by 2017, primarily at the expense of on-premises Exchange.[1]

A recent Dimensional Research2 survey found that 46 percent of respondents (N=202) already used a Software-as-a-Service (SaaS) or cloud-based email solution while 51 percent of those remaining were considering a migration. According to the 2014 eDiscovery Journal Cloud Adoption poll, results focused on large, regulated corporations, the primary motives for a cloud migration appear to be cost, risk, and compliance management of growing corporate data. Even though data security and privacy loss were cited as the dominant concerns slowing down cloud adoption, an overwhelming amount of organizations are considering a migration to Office 365, and utilizing it as a part of their information management portfolio.

Opportunities and challenges of the migration to Office 365

As IT departments embark on data migration and legacy data clean-up projects, legal teams must identify and preserve potentially relevant Electronically Stored Information (ESI) on legal hold, usually by collecting all ESI based on custodial metadata, locations, keywords, or other criteria. Most organizations will have significant quantities of email and files under legal hold when they consider migrating active business files and long-term records to Office 365. A surprising majority of these companies rely on custodians to preserve their own data in unstructured sources. File shares, local computer drives, and other sources do not allow legal or IT to protect loose files and email against inadvertent destruction. Passive reliance on custodians to ‘do no harm’ can only work in systems without automatic retention expiry or other mechanisms that purge files without user approval.

1. Osterman Research Inc., April 2015.

Third-party eDiscovery solutions can be used to automatically map and collect data on legal hold from file shares, custodial mailboxes, SharePoint sites, and other sources. Since large enterprise migrations can take months or even years, incremental and scheduled collection functionality can minimize preservation costs and the risk of losing ESI. These broad preservation collections can be kept on offline storage or archived on-premises or in the cloud for eDiscovery search and retrieval.

By taking a proactive approach in line with bench suggestions on retention and dispositions, legal teams can improve their risk profile through migrations. Here's why: the 2006 Federal Rules of Civil Procedure (FRCP) amendments defined ESI as potential evidence and conservative counsel immediately held everything to meet unclear preservation obligations. Since that time, case-law and subsequent FRCP amendments appears to have made it possible to selectively expire ESI not under hold and to clean up legacy repositories with reasonable process, technology, and documentation.

Legal should embrace the opportunity to engage in the defensible deletion of ESI that is Redundant, Outdated, or Trivial (ROT) in the migration to Office 365 as long as they understand what legal requirements the new system can support and what potential challenges must be addressed.

The legal hurdles of Office 365

Office 365 Gap	Description
No support for journal archiving	Journal archiving lets you capture an immutable copy of all emails sent and received throughout your organization in a secure archive that's kept separate from end user action. Journaling helps ensure full message capture for compliance and eDiscovery purposes–even if an end user deletes or modifies a message, the original, unaltered copy remains in the archive according to your corporate retention policies. Without journaling, it may be difficult to prove that emails weren't tampered with or that items were not deleted. While Office 365 does support journaling, the journaled email must be directed to a third-party archive or external mailbox (an In-Place Archive in Office 365 does not contain journaled items, it is just another mailbox that appears alongside the primary mailbox and gives users a place to store older emails).[2]
End users can delete messages, regardless of applied retention policies	Messaging Records Management (MRM) technology in Office 365 enables organizations to apply retention settings to an entire mailbox and default mailbox folders such as Inbox and Deleted Items to determine how long messages should be retained. However, while the MRM capability ensures that messages are removed after the specified period, it doesn't ensure that messages are retained for the specified period. Employees can still delete messages from their primary mailbox and In-Place Archive before the retention period is reached; MRM isn't designed to prevent employees from deleting their own messages.[3]
To preserve all email, all users must be on legal hold	If you require emails to be retained for a certain period, even if the end user deletes it before that period has lapsed, Microsoft recommends the use of its legal hold functionality (In-Place Hold or litigation hold) to meet this requirement. This functionality is only available in the more expensive E3 and E4 plans. To proactively preserve all email without the journal capability your organization would essentially need to place all users on legal hold.[4]
Information about Bcc and distribution list recipients may not be discovered	Office 365 requires a legal hold on the message to capture distribution list recipients.[5] Without a legal hold, it would be impossible to accurately determine who actually received the email. For example, if an email is sent to the distribution list "All_Finance," it would simply prove that "All_Finance" received the message, but not specifically who was in the distribution list at the time it was sent. The sender would need to be on legal hold in order to capture that information. In addition, information about Bcc and distribution list recipients is stored with the message in the sender's mailbox only.[6] Therefore, it will only be found or displayed if the sender's mailbox is included in the eDiscovery search. For example, imagine Bob (sender) sent an email to Steve (to) and Jack (Bcc). If the search only included Steve's mailbox, the person performing the search will never know that Jack also received the email. They would only see the Bcc information if they included Bob's mailbox in the search.

2. https://technet.microsoft.com/en-us/library/jj898487%28v=exchg.150%29.aspx
3. https://technet.microsoft.com/en-us/library/jj898487%28v=exchg.150%29.aspx
4. https://msdn.microsoft.com/en-us/library/gg271153%28v=exchsrvcs.149%29.aspx
5. https://technet.microsoft.com/en-us/library/dn767952(v=exchg.150).aspx
6. https://technet.microsoft.com/en-us/library/dn770225(v=exchg.150).aspx

Office 365 Gap	Description
Retention policies cannot be applied to inactive mailboxes	With Office 365, whenever an employee leaves the organization, his/her mailbox must be placed on legal hold and converted to an inactive mailbox (an option that is only available in the more expensive E3 and E4 plans) in order to preserve the email.[7] This requires an IT intervention every single time an employee leaves. If the mailbox isn't converted to an inactive mailbox status within 30 days of deletion, the mailbox and its contents will be permanently deleted.[8] The inactive mailbox feature may have very little value in the real world since litigation often takes place months after an employee has left. At the time of your employee's departure, you may have no reason to anticipate litigation, and therefore, no real motivation to convert the mailbox to an inactive mailbox. In this real-world scenario, the emails are lost indefinitely and unavailable for eDiscovery purposes. In addition, retention policies cannot be applied to inactive mailboxes, and if a legal hold duration has been specified, the parameter does not impact inactive mailboxes.[9] Therefore, all content in inactive mailboxes is held indefinitely until the hold is lifted. This may result in the over-retention of emails and an increased scope and cost of discovery.
Limited content support	Office 365 can only preserve (via legal hold) and discover Exchange, SharePoint, and Lync content. For many organizations, archiving and eDiscovery is about more than just Microsoft content.[10] A solution that exists outside of the primary application is the best way to address this inevitable expansion of requirements.
Microsoft cannot guarantee exactly where your data will be stored	While your organizations' country or region determines the primary storage location for your data, the data can be moved to a variety of locations for day-to-day management or backup purposes.[11] This may have implications for organizations under strict obligations to comply with various jurisdictional requirements, such as a requirement that data not leave a particular geographic area.
Siloed cases	Office 365 offers no centralized matter management, dashboard, custodian list, or other functions that track or share criteria, targets, or filters across case sites.
Legal holds are not instantaneous and can require IT involvement	The In-Place Hold and litigation hold setting in Office 365 can take up to an hour to take effect.[12] To preserve large numbers of mailboxes, Microsoft recommends using its litigation hold feature. The litigation hold setting must be managed by IT using the Exchange Management Shell command-line interface or Exchange Administration Center, and preserves the entire mailbox.[13]
No practical legal hold notifications	Office 365 offers no practical legal hold notifications for tracking, custodian acknowledgement or other options.
Limited search criteria	Office 365 offers limited search criteria that relies on manual selection of individual targets. Large lists of terms or phrases (>5,000 characters) may error out. It also has limited search metadata fields.
No role-based security within default site templates	In order to conduct an eDiscovery search, a user must be added to the Discovery Management role group. Members of this group can access sensitive message content in users' mailboxes.[14] Specifically, these members can search all mailboxes in the Exchange organization, preview messages (and other mailbox items), copy them to a discovery mailbox and export the copied messages to a .pst file. Many customers might recoil at putting this level of global search access into the hands of all discovery managers. It is possible to create custom management groups to let specific users search only the mailboxes of employees who are members of a specified distribution group. However, this is not the default process, and requires IT intervention.[15]
No early stage culling or review functionality	Office 365 seems to support a "pump and dump" approach to eDiscovery, predicated on broad-based search and exporting the results for external legal review. It does not offer any real level of early stage culling or review functionality. To review search results, they must either be exported to a third party eDiscovery tool or copied to a discovery mailbox and reviewed in Outlook or Outlook Web App (OWA).[16] Using Outlook or OWA as the review tool makes reviewing large quantities of search results or sharing review responsibilities across groups of people largely impractical, and introduces significant risks of metadata alteration or loss. There is no hit-highlighting of the returned search results. Consequently, a review of hundreds or thousands of items becomes more difficult when the reviewer must read each item without the aid of hit-highlights. The only way to "organize" items is to make copies or manually move them into new folders within the discovery mailbox. With no intelligent way to classify the data and redact unwanted and irrelevant content, you potentially risk exposing sensitive and privileged data as well as over-producing content which may increase your legal fees.
Limited export speeds	Office 365's export speed is limited to 1.25-2 GB/hour, based on Microsoft estimates and testing. Normal custodial volume exports could take weeks per case.

7. https://technet.microsoft.com/en-us/library/dn770225(v=exchg.150).aspx
8. http://blogs.technet.com/b/exchange/archive/2013/03/21/preserve-mailbox-data-for-ediscovery-using-inactive-mailboxes-in-exchange-online.aspx
9. http://blogs.technet.com/b/exchange/archive/2013/03/21/preserve-mailbox-data-for-ediscovery-using-inactive-mailboxes-in-exchange-online.aspx
10. http://blogs.technet.com/b/exchange/archive/2013/03/21/preserve-mailbox-data-for-ediscovery-using-inactive-mailboxes-in-exchange-online.aspx
11. https://technet.microsoft.com/en-us/library/dd298021%28v=exchg.150%29.aspx
12. http://technet.microsoft.com/en-us/library/dd979797(v=exchg.150).aspx
13. http://technet.microsoft.com/en-us/library/ff637980(v=exchg.150).aspx
14. http://technet.microsoft.com/en-us/library/dn741464(v=exchg.150).aspx
15. https://technet.microsoft.com/en-us/library/dd298021(v=exchg.150).aspx#discmbxs
16. http://technet.microsoft.com/en-us/library/dn741464(v=exchg.150).aspx

With corporate IT pushing Office 365 pilots and adoption, legal departments must find mature solutions to meet their critical requirements for legal holds, collection, ECA/investigations, review, and productions. The first generation of the eDiscovery Center raises concerns for enterprise customers with real world discovery, compliance and regulatory requests.

Enterprises and government agencies require a centralized solution for managing all aspects of eDiscovery related to their litigation, regulatory inquiries, and investigations and legal departments can benefit from a single platform to manage, track, and coordinate their discovery response efforts.

That does not mean that the eDiscovery Center cannot play a role by providing broad In-Place preservation or scoping simple search terms. These functions should be managed and tracked from your central eDiscovery solution as a small part of the overall discovery process.

Veritas archiving and eDiscovery–supplementing Office 365

Veritas offers market-leading archiving and eDiscovery solutions that integrate with Office 365 to enable legal teams to meet their key preservation and discovery obligations.

Veritas™ Enterprise Vault.cloud

Veritas™ Enterprise Vault.cloud is a leading cloud-based archiving service that integrates with Office 365 to provide the essential layer of functionality you need to meet the rigorous business and regulatory demands for preserving data and ensuring rapid eDiscovery search and review. Its intuitive eDiscovery Web interface provides legal teams and outside counsel with direct, roles-based access to the archive, where they can interact and collaborate on legal, regulatory, and investigative matters–with no help from IT required.

- **Satisfies email retention requirements** by journaling an immutable copy of every email sent and received to a secure and tamper-proof cloud-based archive.
- **Archives content beyond Office 365** including Microsoft® Exchange Server and IBM Domino® emails, Box, and Microsoft SharePoint® Server files, instant messages, and unified communications.
- **Grants granular, roles-based access and permissions**, allowing those involved in an eDiscovery case to perform functions such as managing searches, reviewing items, and creating exports.
- **Provides a complete understanding of who sent and received a message** by automatically capturing Bcc and distribution list recipient information which is discoverable during searches of both the sender and recipients' archives.
- **Enables powerful, iterative searches across an unlimited number of custodians** (search within a search), allowing users to add and remove search filters "in progress" until they achieve the desired dataset.
- **Quickly narrows down eDiscovery search results** with built-in collaborative early stage culling and review capabilities, which can save considerable legal expenses down the road.
- **Directly integrates with Veritas™ eDiscovery Platform** which supports collection and review of content from both inside the archive and outside in non-archived sources (add-on option).
- **Provides end users with seamless access to their archived information** directly from Outlook (and IBM® Notes), mobile devices, and Web browsers.

- **Reduces the risks associated with migrating to Office 365** by archiving legacy data first and ensuring chain of custody throughout the ingestion process.
- **Mitigates the risks of holding data with a single vendor** by providing the reassurance of a secondary copy of ESI in another location.

Veritas™ Enterprise Vault

Veritas™ Enterprise Vault is a leading on-premises archiving solution that directly supports SMTP journaling from Office 365 directly to the archive, without the requirement for journal mailboxes. In this way, Enterprise Vault may be maintained on-premises to support compliance, supervision, and/or eDiscovery requirements, even with email in the cloud with Office 365.

- **Satisfies email retention requirements** by journaling an immutable copy of every email sent and received to an on-premises archive.
- **Archives content beyond Office 365** through native integration and an expansive technology partner ecosystem, including email, instant messages, SharePoint, file systems, structured data, social media, and more.
- **Provides end user access to archived information** from Outlook, browsing and federated searching capabilities across archive sources, and offline access to archived messages via advanced local caching.
- **Supports the use of retention folders** to enable end users to manually classify and retain content, as well as automated classification, retention and tagging of Exchange email for expanded search and supervisory review.
- **Supports core corporate eDiscovery workflow requirements for archived content** via the entry-level Enterprise Vault Discovery Accelerator (add-on option).
- **Directly integrates with eDiscovery Platform** which supports collection and review of content from both inside the archive and outside in non-archived sources (add-on option).
- **Reduces the risks associated with migrating to Office 365** by archiving legacy data first and ensuring chain of custody throughout the ingestion process.
- **Mitigates the risks of holding data with a single vendor** by providing the reassurance of a secondary copy of ESI in another location.

eDiscovery Platform

The eDiscovery Platform was purpose-built for eDiscovery and supports the entire corporate eDiscovery lifecycle from legal hold and collections through analysis, review, and production. It is available as a physical or virtual appliance that provides enterprises, government agencies, and law firms a single interface across all of their key data assets.

- **Can be used to automatically map, collect, and manage ESI** in legacy repositories and in Office 365 simultaneously in one user interface. This minimizes the impact to the discovery team and enables continuity through the migration process and beyond.
- **Provides centralized matter management** capabilities to enable you to manage all of your cases from one dashboard.
- **Provides a data map** to help you track and manage your key ESI sources.

- **Manages hold notices** through creation, responses, and automates reminders directly connected to your case with custom templates to ease the burden and manage risk.
- **Broad and federated collection** from over 50 enterprise data sources. The solution can collect from many different data repositories whether on-premises or in the cloud. Federated collections execute immediate or scheduled collections across all key ESI sources with full integrations to desktops, file shares, SharePoint, Exchange, Enterprise Vault archives, Enterprise Vault.cloud archives, and Office 365 mailboxes/SharePoint sites.
- **Allows customers to bypass Office 365's collection chokehold** with multithreaded connectors for practical collection rates. Exports on-demand from Enterprise Vault.cloud to meet tight deadlines.
- **Selective preservation** that enables customers to collect from Office 365 to meet the higher preservation requirements of criminal investigations and some regulatory requests.
- **ECA and investigations** enable search and review ESI from key custodians to assess risk and support relevance scope definition. Manage costs and volume upstream.
- **Secured preview** which enables direct access for review by outside counsel, experts, and regulators to bypass the time and expense of third-party processing and hosting.
- **Advanced machine learning called Transparent Predictive Coding** that cuts the time and cost of review by inside/outside counsel while improving quality and consistency.
- **Full processing and production capabilities** that convert native files to requested TIFF, text, and load files. TIFF on the fly enables manual and automated redactions to protect confidential and privileged content.
- **Offers a wide range of search filters and data analytics** available across search results. In the eDiscovery platform users can build a 100-line search query, each line containing a maximum of 8,000 terms. The search will include all indexed content including metadata, within zip files, within attachments, etc. for the 500+ supported file types. The platform also offers concept clustering, facet navigation, social network analysis, chronological analysis, and more without additional fees.
- **Pre-defined system level role-based users are included.** In addition these roles or custom roles can be added to define permissions allowing access to the entire system down to a single document within a single case.
- **Rapidly cull non-relevant information** leveraging a wide range of tools like auto-filters, Transparent Keyword and Concept search and predictive coding prioritization.
- **Fast export speeds** that start in the 10's of GB per hour and can be scaled out if more performance is needed.

Conclusion

A surprising majority of organizations are either considering or adopting Microsoft Office 365. Legal needs to be involved in every step of potential migrations to ensure that ESI under hold is preserved and that their discovery requirements can be met in the final solution design. Although Office 365 has a number of key functional challenges, these can be addressed by mature archiving and eDiscovery solutions by leading market providers such as Veritas. The combination of the eDiscovery Platform, Enterprise Vault.cloud, and Enterprise Vault represents a unified solution that addresses most customers proactive and reactive compliance and eDiscovery requirements while managing the cost and risk associated with out of control data growth.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21351023 05/2015