Enterprise Vault White Paper

Archiving and eDiscovery of Social Media and Instant Messaging

This document is to provide an overview of the Enterprise Vault social media and instant messaging archiving solutions that are available through Symantec partnerships.

If you have any feedback or questions about this document please email them to **IIG-TFE@symantec.com** stating the document title.

This document applies to the following version(s) of Enterprise Vault: 10.x

Document Control

Contributors

Who	Contribution
Liam Finn	Originator
David Scott	Contributor
Ron Ruggles	Contributor
Allison Walton Esq.	Contributor

Revision History

Version	Date	Changes
V1.0	3/27/2012	Initial release
V2.0	7/20/2012	Added details on compliance regulations affecting Social Media and IM archiving Added info on partner contacts and licensing Added decision matrix to assist in choosing partner solution
V2.1	11/20/2012	Update new content sources

Related Documents

Version	Date	Title

Table of Contents

Introduction

Social media is attracting a great deal of attention due to recent guidance from FINRA, IIROC and (in the UK) the Financial Service Authority. These agencies are mandating the protection of social media and clarifying that financial service companies must preserve this content in the same manner that they preserve email and other online communication. While some companies continue to simply ban social media, the majority are starting to embrace social media use internally and externally and are looking for guidance on how to safety implement a social media strategy.

In this white paper, we will cover three key areas:

- How does social media and Instant Messaging [IM] archiving work from a technical point of view
- Capabilities and differentiators of four key Enterprise Vault [EV] partners
- Legal and regulatory considerations

Further details on the regulatory bodies and their present policies surrounding social media and IM archiving and eDiscovery requirements can be found in the **Laws and Regulations that affect social media archiving and eDiscovery** section of this paper

How does social media / Instant Messaging archiving work?

Deployment models

Symantec has partnered with several solution providers to facilitate capture of social media and instant messaging. Depending on the solution it may be deployed on-premise or in the cloud as shown in Figure 1.

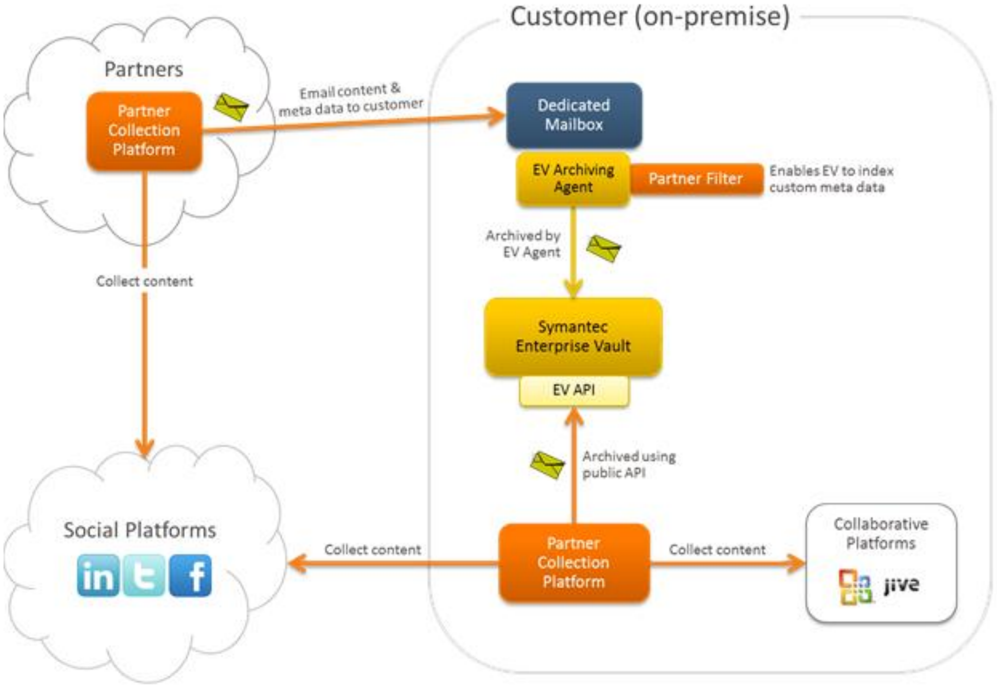

Figure 1 – Deployment models

In the following sections we will look at each of these options and discuss the pros and cons of each solution.

On-premise

An on-premise solution requires that either a partner's appliance or a server with the partner's software is installed, and this performs the collection of the data from any on-premise enterprise collaboration solutions (Jive, Yammer, Chatter), social media (e.g. Twitter, Facebook, LinkedIn) and both internal and public instant messaging providers (Microsoft Lync, Lotus Sametime, Yahoo Instant Messenger, MSN Messenger, Jabber etc.)

This solution also offers the additional advantage of being able to leverage the EV Content Management API and archive the content directly into an onsite EV archive. This has many advantages as there are fewer steps involved in the solution, and no Journal Mailbox is required. Leveraging the Content Management API allows the vendor to capture additional metadata into Enterprise Vault, which can be used when searching the content.

Not all on-premise solutions leverage the API; some use SMTP to send the captured content to a journal mailbox, where it is then archived by Enterprise Vault.

Cloud / SaaS

Cloud / SaaS solutions provide faster deployment by not requiring any hardware installed on site. They still have the ability to send the captured content to EV in the form of an email. This email is directed to a dedicated mailbox, which is archived using the EV Journaling task. Partners adopting this method of integration should create a "Journal Filter" plugin to be installed in EV, which will enable EV to index the metadata name/value pairs to allow searching by the Clearwell eDiscovery Platform or Discovery Accelerator. If a Journal Filter is not in place, the sender/recipient, subject and date will be captured from the email.

Capture methods

There are three primary methods used today to capture social media and instant messaging content:

Proxy

Proxy-based solutions provide the ability to capture real-time data as it is accessed, created or written to social media. This method provides more manageability of what content is created, thereby providing the ability to restrict features or restrict access to groups within the company. This method only works on content created while within the network of a company or when using a laptop/tablet that has modified the proxy settings for internet browsing to pass through the proxy. It does not have any ability to capture information written or accessed from devices that can have independent access to the Internet such as cell phones or other mobile devices.

Proxy based solutions provide the ability to

- Restrict use of social media, collaboration and IM entirely on a per-application basis
- Restrict access to individual social media features on a per-user basis
- Prevent specific content from being posted
- Restrict access to specific internal groups or individuals

In most cases, the proxy solution is used either by:

- a monitoring port on an Internet choke switch inside the company firewall
- a DNS redirection to have all requests to a particular social media site or instant messaging provider redirected to the internal server / appliance used to capture the content, which then acts as a relay to the outside content provider.

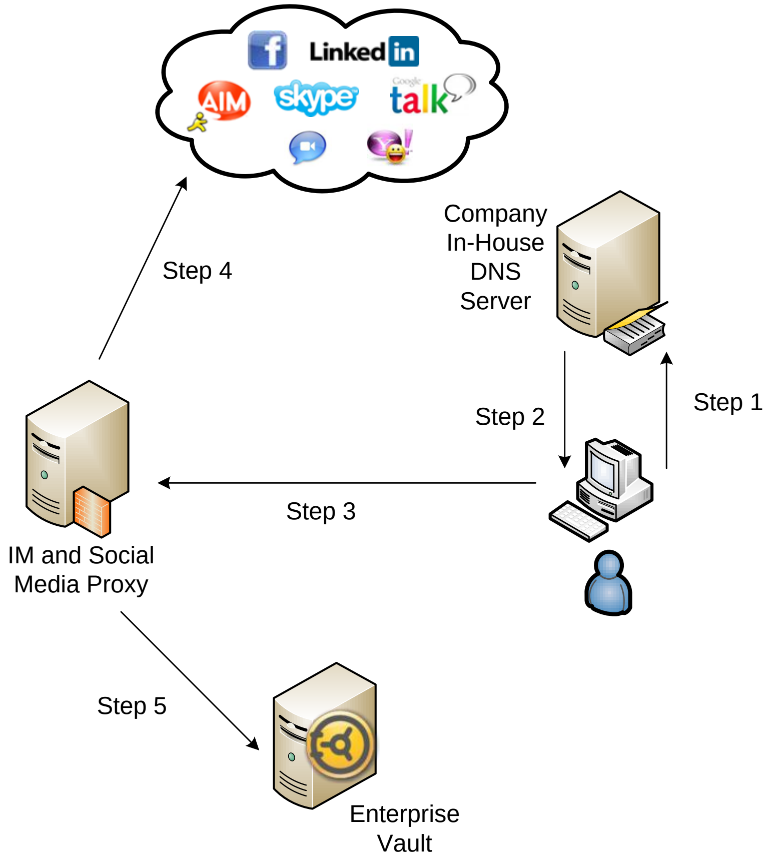

Figure 2 – Proxy method

1. User tries to connect to instant messaging or social media provider and send DNS request to in-house DNS to resolve the name.
2. In house DNS server returns the IP of the partner provided proxy appliance / server.
3. Client application connects to the proxy server which first checks access policy to grant or deny access and then relays the authentication requests the cloud social media or instant messaging provider.
4. Connection is made to cloud provider via the proxy device. All communication to the cloud provider is captured real time as it passes through the proxy device.
5. Proxy device sends content to EV via API or packages content into an email and sends it to a Journal mailbox to be archived.

API

API based solutions leverage the social media's native API to capture all content and often is managed by installing a small application within the page to monitor content changes. This method does require end-user access to the page.

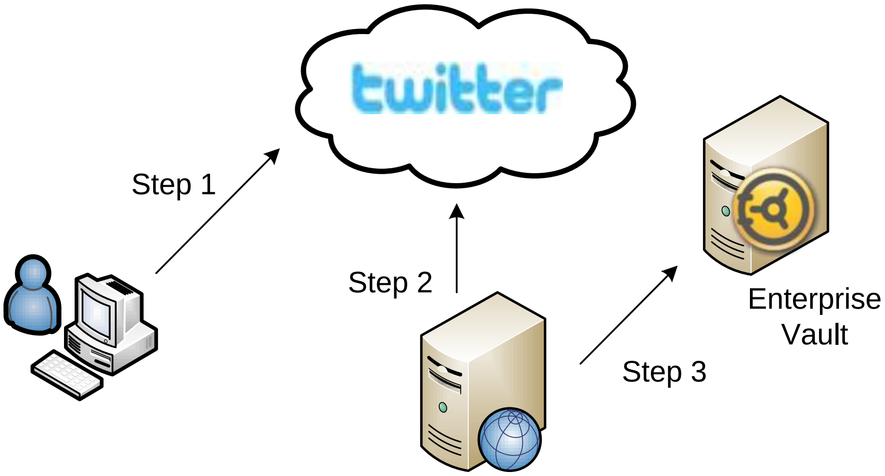

Figure 3 – API Twitter query

Twitter Search API

Twitter is archived using the Twitter search API, which provides the ability to run searches against Twitter content. This has a limitation that on average you can only search 6 – 9 days of history. For this to be effective, the API needs to run on a regular basis to ensure no tweets are missed.

1. User posts to twitter
2. Partner utilizes twitter search API to gather content
3. Content is then packaged into an email and sent to a journal mailbox for archiving by Enterprise Vault. Some partners can write direct to EV using the Content Management API if they have an onsite presence.

LinkedIn API

To archive the content of LinkedIn, Symantec's social media archiving partners leverage the LinkedIn API. This API grants them access only to pages they have been authorized to query. The API uses the OAth authentication protocol to connect to LinkedIn and retrieve the data. Two keys are required to grant access to the page or profile so its content can be read using the API. They are the API key and secret key which are assigned to the partner by LinkedIn. Then a request is made by the partner for access to the content to be archived. Once this access is granted, the partner can then initialize content collection.

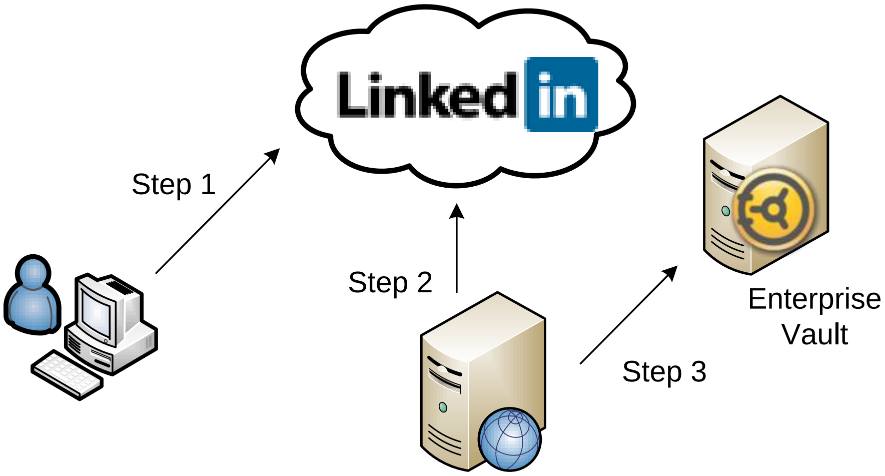

Figure 4 – LinkedIn API

1. User posts to LinkedIn.
2. Partner utilizes LinkedIn API to gather content using appropriate security.
3. Content is then packaged into an email and sent to a journal mailbox for archiving by Enterprise Vault. Some partners can write direct to EV using the Content Management API if they have an onsite presence.

Facebook Graph API

The Symantec Social Media partners generally utilize the Facebook Graph API to archive the contents. To use the Graph API, an application should be created and granted full access to the Facebook page.

Once granted access, the partner can leverage the API to gather data direct from the Facebook page. The process is similar to the LinkedIn API but utilizing the Graph API for Facebook instead.

Crawling

Crawling is the ability to look at the content over the web and read what is on the site such as Facebook or Twitter. During the crawl, the content is captured, but the downside of this is that access needs to be granted to the site such as making the vendor a friend on Facebook or being a follower on Twitter. As crawling runs on a schedule, there is a chance that data may change between the crawls and therefore can be missed. This does not work for instant messaging solutions as the majority of instant messaging solutions are person-to-person and session dependent, so there is no history viewable via a web interface to capture unless you are part of the initial conversation.

Archive to EV

The archiving of content into EV has strict guidelines that the partners must meet to provide basic information, so EV can correctly understand the content and index it in the correct manner. EV's method of archiving the captured content is done by having the partners package the captured content into an email. This message must also have the original items attached to the email for eDiscovery reasons.

Message structure

There is a basic message structure required to allow the archiving of this content. The Message envelope contains what you normally expect to see in the header information of an email such as To, From, Subject and so on. The message body contains the content of the original item and is either plain text or HTML. This is the content that is indexed by Enterprise Vault.

Attachments may be included which will contain the original data as collected by the partner application. For example one of our partners – Hanzo – provides a PDF representation of the content as an attachment.

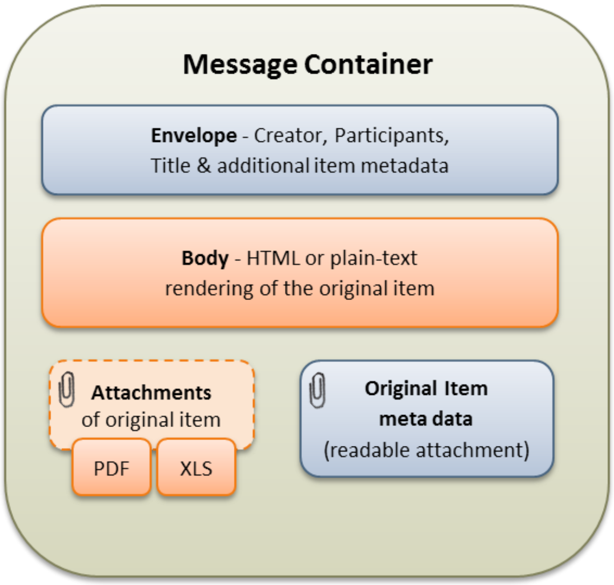
Message Container
Envelope - Creator, Participants, Title & additional item metadata
Body - HTML or plain-text rendering of the original item
Attachments of original item
PDF
XLS
Original Item meta data (readable attachment)

Figure 5 – Message structure

Partners may include an item meta data attachment contains the Item Type (Facebook, Wiki etc.) as well as the original Item meta data (Created Date, Modified By, etc.). This content is also indexed by EV and become searchable items for eDiscovery purposes.

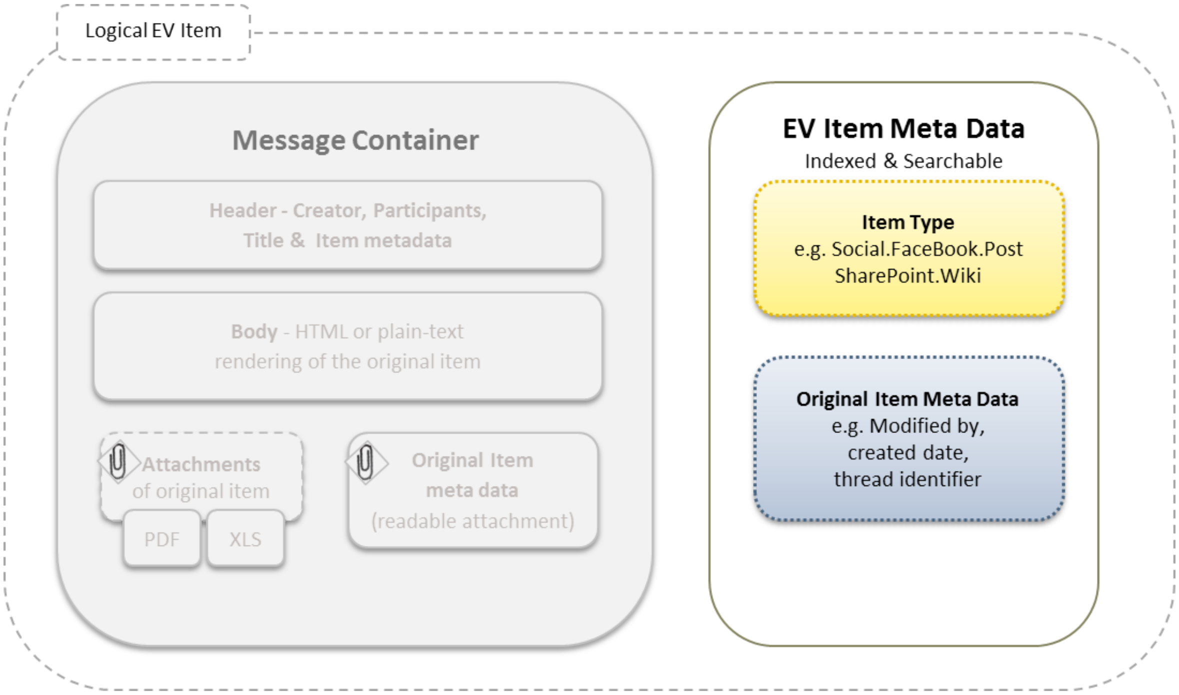
Logical EV Item
Message Container
Header - Creator, Participants, Title & Item metadata
Body - HTML or plain-text rendering of the original item
Attachments of original item
PDF
XLS
Original Item meta data (readable attachment)
EV Item Meta Data
Indexed & Searchable
Item Type
e.g. Social.FaceBook.Post
SharePoint.Wiki
Original Item Meta Data
e.g. Modified by,
created date,
thread identifier

Figure 6 – Metadata structure

Metadata mapping

Symantec's social media and IM partners must extract name value pairs to allow proper searching within the Clearwell eDiscovery Platform. Metadata can be extracted upon ingestion by partners using the API direct ingest method. Partners who send content via a Journal Mailbox will need to create a "Journal Filter" to extract metadata into EV.

One of the key fields that must be set is the Vault.MsgType attribute. This is normally set by EV automatically when ingesting content. In the case of social content, the partner will set this attribute if they choose to directly ingest into EV via our published APIs. If they are using the Journal Mailbox method, the partner can set this via an x-header. This will allow filtering the search based on "Message Type" in the Clearwell eDiscovery Platform.

Other fields will also be mapped to standard EV fields for Author, Title, Date, etc. Other metadata that does not map directly to EV fields can be added by the partner as custom attributes.

eDiscovery

How to discover this content

Discovery against social media and instant messaging archived data is identical to discovery against email content. This is because social media and instant messaging content is archived by EV as an email item.

Starting with the Clearwell eDiscovery Platform version 7.1.1, social media and instant messaging content ingested via a journal mailbox and stored within EV can be directly ingested into Clearwell.. The system will leverage the translated metadata fields to query the content just like any email.

Even though EV can index custom metadata, the ability to search this data is not available at present in the Clearwell eDiscovery Platform.

Export and production

Exporting social media and instant messaging content needs to comply by the same rules used to export emails. They can be exported as EML which can be rolled up into an NSF or as MSG files which can be rolled up into PST files. This also includes the attachments which we discussed earlier. Producing the content must include the attachments because the attachments are the original item and its original metadata.

Solution providers

Since there are a growing number of social media and IM solutions, Symantec has partnered with four of the leading solution providers to provide our customers with archiving from a broad range of Social media or IM content sources. Below is a list of the partners that Symantec works with to provide the best all round solution for an organization's archiving needs.

Partners at a glance

This shows a list of the partners and the solutions each provides.

Partner	Actiance	Globanet	Hanzo Archives	Socialware
Product Name	Socialite and Vantage	Merge1	Archive	Compass
Type of Solution	Capture and Control	Capture	Capture	Capture and Control
Collection Method	Proxy and API	API	Crawl	Proxy and API
Deployment	Appliance, SaaS and On-Premise	On-Premise	Appliance, SAAS	SAAS

Table 1 – Social media capturing partners

Who can archive what

Table 2**Error! Reference source not found.** provides a listing of the content that each partner can archive. This listing should be leveraged in conjunction with your Symantec Account Manager to decide which solution best fits your needs.

NOTE: This list is subject to change without notice as partners add or remove content sources at their discretion.

Source Content	Actiance	Hanzo Archives	Socialware	Globanet
f	✓	✓	✓	✓

Source Content	Actiance	Hanzo Archives	Socialware	Globanet
LinkedIn	✓	✓	✓	✓
twitter	✓	✓	✓	✓
YouTube	Coming Soon	✓	✗	Q1 2013
flickr	✗	✓	✗	✗
yammer	Coming Soon	✓	✗	✓
chatter	Coming Soon	✓	✗	✓
Google+	✗	✓	✗	Q3 2013
jive	✓	✓	✗	✗
Microsoft SharePoint 2010	✓	✓	✗	✗
Websites	✗	✓	✗	✗
Microsoft Lync	✓	✗	✗	✓
Microsoft Office Communications Server 2007	✓	✗	✗	✓
AIM	✓	✗	✗	✗
Bloomberg	✓	✗	✗	✓
REUTERS MESSAGING Thompson Reuters	✓	✗	✗	✓
skype	✓	✗	✗	✗
Y!	✓	✗	✗	✗

Source Content	Actiance	Hanzo Archives	Socialware	Globanet
Lotus Sametime	✓	✗	✗	✗
Lotus Connections	✓	✗	✗	✗
Pivot IM Trader	✓	✗	✗	Supported via an XML Connector)
YellowJacket	✓	✗	✗	✗
Apple iChat	✓	✗	✗	✗
Cisco Unified Presence Server Cisco Jabber	✓	✗	✗	Q2 2013
Google talk	✓	✗	✗	✗
Microsoft/Parlano MindAlign	✓	✗	✗	✗
UBS Chat	✗	✗	✗	✓
SkyTel	✗	✗	✗	✓
XIP	✗	✗	✗	✓
Merrill Chat	✗	✗	✗	✓
LiquidNet	✗	✗	✗	✓

Source Content	Actiance	Hanzo Archives	Socialware	Globanet
TRADEWeb	✗	✗	✗	✓
spigit	✗	✗	✗	✓
BazaarVoice	✓	✗	✗	✓

Table 2 – Capture ability by partner

Actiance

Actiance offers two solutions:

www.actiance.com

Actiance offers two solutions:

Socialite

Socialite provides a proxy solution which captures content in real-time as posts are made. This also captures the pages a user has viewed and any content created, modified or deleted. The proxy-based solution also allows control of social networking by providing control over access to social media and granular control over features within each social app (e.g. turn off "Like" in Facebook).

Socialite also leverages API-based capture to provide complete protection even when outside the office environment. API-based capture takes snapshots of Facebook, LinkedIn and Twitter at various times during the day. Snapshots will be threaded together to eliminate duplication. This allows each conversation to be archived into Enterprise Vault as a single item which is more efficient than capturing each individual post/reply.

Socialite can be implemented as a hosted or on-premise solution.

Vantage

Vantage provides an in-stream proxy solution which captures instant messaging conversations in real time. It also offers the ability to manage access to instant messaging and user mapping to instant messaging alias.

Vantage is also used to capture corporate social content solutions such as Lotus Connections (currently sold only via IBM) and Jive. They plan to expand internal social media via Vantage in the near future.

Once content has been captured from either Vantage or Socialite, it is emailed to a Journal Mailbox using the SMTP export feature and archived by a Journaling task in Enterprise Vault. Actiance is working on a Journal Filter to extract metadata which is targeted for fall 2012.

Hanzo Archives

Archives

This is the solution from Hanzo Archives which provides web / social media archiving. They do not offer an instant messaging solution. It is deployed as an appliance or as a SaaS solution. Hanzo Archives crawls target websites and collects the content into its native archive on a schedule. The content in the archive is stored in native format and not linked back to the source site, so the content once collected is static and looks exactly as it did at the moment of collection. The integration into EV is also unique as they send a rendered copy of the item into the archive as an email message so it can be indexed; inside the message there is a link which connects the user to the item in the Hanzo Archives where they can view the content. Hanzo Archives also includes a PDF representation of the original item and an attachment to show all the metadata captured with the item which makes it searchable within EV. Hanzo Archives is the only partner to provide web-site archiving.

Socialware

Compass

The solution from Socialware is for social media only and is provided as a SaaS solution that provides all the necessary compliance requirements to meet FINRA regulations. This includes policy, moderation of the content, and archiving of the content for eDiscovery needs. Compass is a proxy and API based solution that can provide granular access controls to LinkedIn, Twitter and Facebook allowing the enabling/disabling of specific features on a per-user basis. Socialware is primarily focused on the financial industry and provide both a proxy-based and API-base capture/control solution. Socialware and Actiance are the only major players that provide both proxy and API based control/capture.

Globanet

Merge1

Merge1 is an on-premise solution which leverages an API approach to collection from solutions such as Twitter and Facebook as well as onsite instant messaging solutions. For Twitter it leverages the Twitter search API, and for Facebook it uses the Graph API.

Merge1 also provides connecters to some onsite instant messaging solutions such as Microsoft Lync and Microsoft Communication Server etc. It does not support the collection of public instant messaging such as Yahoo Instant Messenger or MSN Messenger. Globanet plans to add support for LinkedIn, Yammer and Chatter in July 2012.

Choosing a Partner

Choosing a partner is one of the most critical decisions to be made. The choice of partner will depend on the organization's needs. For example, decision criteria may include:

- Hosted or on-premise

- Do they need to block access to networks or block specific features or do they just want to capture content?
- IM archiving – do they need to archive Instant messages and if so what IM solutions do they need to support?
- Social Media & Collaboration networks required – Different partners provide different capabilities as evidenced by the chart shown above. Customers need to ensure the partner they select matches the networks they need to collect.

Table 3 summarizes some of the key areas of differentiation between partners:

Criteria	Actiance	Globanet	Hanzo Archives	Socialware
On Premise	✓	✓	✓	✗
Hosted	✓	✗	✗	✓
Method of capture	API/Proxy	API	API/Proxy	Crawler
Block/Moderation	✓	✗	✗	✓
Instant Messaging	Most are supported	Microsoft Lync only	✗	✗

Table 3 – Partner summary

Licensing

Enterprise Vault

When archiving into EV from a Partner application, a license for the EV Custom Archiving Agent is required for each Terabyte of ingested content.

Partner licensing and contact

Each of Symantec IM and social media archiving partners has their own method of licensing. While delving into each of these partners' individual licensing requirements is outside the scope of this document, a brief outline can be found in Table 4

Partner	Licensing Model	Contact Email	Contact Phone	Website
Actiance	User Based	info@actiance.com	(888) 349-3223	www.actiance.com
Globanet	Social Media is based on total number of employees. All other connectors is user based.	sales@globanet.com	(888) 427-5505	www.globanet.com
Hanzo Archives	Licensing model depends on source type and scope of the collection. Contact Hanzo Archives directly for details.	contact@hanzoarchives.com	(415) 692-5425	www.hanzoarchives.com
Socialware	The pricing is on a user not capacity basis. SaaS model with per seat, per month pricing at enterprise level	info@socialware.com	(512) 329-8880	www.socialware.com

Table 4 – Partner licensing and contact information

Laws and Regulations that affect social media archiving and eDiscovery

The proliferation of social media usage has made it as commonplace as email and is now a primary form of communication both inside and outside of the workplace. Social media users are addressing personal and work related topics by posting content as they travel to and from social media sites. The cross-over between personal and professional social media usage has blurred the lines regarding what may be discoverable in the litigation context and what the appropriate level for an expectation of privacy for users of social media should be.

A recently commissioned Symantec **survey** found that over the period of one year, the typical social media incident costs a company approximately 4 million dollars. Concerns about employees posting confidential information, data loss, litigation exposure and brand damage were among the top concerns companies have with 94 percent suffering negative economic consequences. The data explosion in conjunction with the technical challenges social media presents across the **Electronic Discovery Reference Model** have further complicated the discovery of this content.

The Stored Communications Act

The Stored Communications Act (SCA) is a federal law that provides the back drop for the discoverability of social media and addresses the disclosure (voluntary or compelled) of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). Enacted in 1986 as part of the **Electronic Communications Privacy Act** (ECPA), the SCA is largely outdated as it has not been modified since the advent of social media.

The SCA serves to limit what digital content a third-party service provider may disclose to a requesting party. The SCA covers two types of providers: (1) electronic communication services (ECS), and (2) remote computing services (RCS). The distinction between the two lies in the amount of time a communication has been in storage, and whether or not the communication has been opened. For the purposes of the discovery of social media in civil lawsuits, subpoenas may be issued to internet service providers (ISP) and discovery of communications are ultimately either compelled by court order, consent is obtained from the user allowing direct discovery, or discovery is denied in part or in whole by the court.

Case law

Since the advent of social media, there have been numerous inconsistently decided cases regarding the discovery of social media that demonstrate this is still a very nascent area of the law. Historically, these cases have been employment law and personal injury focused, but that is changing as social media usage grows both in both personal and professional use cases. It is important to understand the different levels of social media usage that exist and that content may be discoverable in litigation, regardless of a user’s privacy settings. Social media users may have their own personal accounts, may have personal and/or corporate accounts that they use for dual business and personal purposes, and organizations may have their own accounts that result in a social media persona. In all three of these scenarios, social media may be discoverable, and each scenario presents **risks**.

In *Crispin v. Audigier (C.D. Cal.) (May 26, 2010*), the court considered whether or not Facebook messages and wall posts were discoverable in a civil suit under the SCA. The court held that messages that were not posted publicly were in fact protected under the SCA and not subject to production. Conversely, the *E.E.O.C. v. Simple Storage Management LLC (S.D. Ind.) (May 11, 2010)* and *Ledbetter v. Wal-mart Stores, Inc. (D.C. Colorado) (April 21, 2009)* cases illustrate that the SCA does not always protect civil litigants' privacy from and that evidence reasonably calculated to lead to relevant information may be subject to discovery. In *People v. Harris*, *(N.Y. Crim. Ct.) (Apr. 20, 2012*), the court found that Twitter messages were discoverable, as they carry with them no expectation of privacy evidenced by Twitter's user-agreement.

The Federal Rules of Civil Procedure

A key legal concept regarding social media involves "possession, custody and control" pursuant to the **Federal Rule of Civil Procedure 34 (a) (1)**. Part of an analysis about the discoverability of social media may depend on whether the information is in the possession, custody or control of the producing party. While users have the right to post, modify, and delete information on most social media sites, it is also true that unless the social media site is internal and hosted on the company's servers, much of the data and metadata regarding communications is hosted by a third party ISP.

This makes the collection of social media different than information within the organization's own IT systems and requires technology to monitor, capture, preserve and to ultimately perform other discovery related analyses. Courts have held that if an organization has access to documents to conduct business, it has possession, custody or control of those documents for the purposes of discovery. This requires that an organization address how they will monitor, preserve, collect and review social media should they need to as technically, the information is beyond their firewalls. Many non-regulated industries have not dealt with the collection of social media, but the issue is imminent.

Additionally, because of authenticity and the metadata capture issues, an exported log of Facebook activity performed by a user would be unsuitable for litigation when metadata is in question. In cases where it is not at issue, courts are expanding the discovery of social media on relevancy grounds. In *Thompson v. Autoliv ASP, Inc. (D. Nev.) (June 20, 2012),* the Plaintiff was ordered to produce *five years* of social media content to opposing counsel for review, as much of the evidence publicly available was contrary to the Plaintiff's initial production.

On a basic level, organizations can begin to take control over their social media environments by completing the following exercises:

- Assess which laws apply to their industries,
- Assess IT systems that are in place through data mapping and review records management and document retention policies,
- Create a social media policy addressing usage and penalties for employees' non-compliance
- Integrate the social media policy into the document retention policy,
- Implement archiving and in-house eDiscovery capabilities,
- Create a plan for litigation including third party partners where necessary,

- Develop a training plan, audit and refresh that training regimen on a consistent basis to guarantee employee understanding and compliance,
- Review by Legal of all user-agreements for social media websites employees are permitted to use,
- Ensure the technology deployed effectuates the written policies in place through testing,
- And finally, deploy data loss prevention technology that will protect the organization by the monitoring of social media risks.

Case law is not the only source of guidance regarding social media regulation. Heavily regulated industries, like the financial and insurance industries, have been amongst the first to issue guidance on how to regulate the use, monitoring, archiving, and collection of social media. While the financial services industry is by far the most developed in the policy and regulation arenas, increasingly companies are integrating their social media policies into their document retention policies as part of a larger information governance initiative. As social media use becomes more commonplace, it is perceived as just another form of data and should be treated as such.

FINRA

The Financial Industry Regulatory Authority **(FINRA)** in the U.S. and the Investment Industry Regulatory Organization of Canada **(IIROC)** are examples of two regulatory bodies that have issued guidance on social media usage and management of content. FINRA is a non-governmental self-regulated organization (SRO) that serves as the enforcement arm of the New York Stock Exchange and **replaced the National Association of Securities Dealers, Inc. (NASD) in 2007**. FINRA works in conjunction with the **Securities and Exchange Commission** to regulate the financial services industry. As technology forges ahead, regulatory bodies are in the process of merging old and new rules to streamline a framework for best practices for ESI and to protect investors as well as the public interest.

FINRA Regulatory Notices 10-06 and 11-39 outline how financial companies and their professionals should use and preserve social media content. Notice 10-06, *Social Media Web Sites,* was issued by FINRA in 2010 and was later expounded on with Notice 11-39, *Use of Personal Devices for Business Communications* in 2011. Emerging “Bring Your Own Device” (BYOD) trends in the workplace, coupled with Notice 11-39’s direction that the content of communications are determinative, and not the medium by which they are communicated, have resulted in the vigilant monitoring of social media to ensure compliance through new technologies. IRROC issued Notice-0349 in 2011 and mirrors FINRA’s record keeping requirements in Canada.

Notice 10-06 outlines the differences between dynamic (does not inherently require approval by a registered principal) and static content (deemed an advertisement requiring approval by a registered principal). FINRA’s 10-06 Notice requires that broker-dealer communications relating to business must be retained and easily accessible pursuant to sections 17a-3 and a-4 of the Securities and Exchange Act of 1934 (SEA) (Record Keeping) and National Association of Securities Dealers (NASD- now FINRA) Rules 3010 (Supervision) and 3110 (Books and Records).

There are other important regulations pertaining to social media use by financial firms. Notably, NYSE Rules 440 (Books and Records) 472 (Communications with the Public) which regulate public communications with investors and requires that communications and research reports be approved prior to release in the market as another layer of regulation for firms that are also members of the New York Stock Exchange. With a projected effective date of February 2013, the **SEC** has approved **FINRA's proposed *New Rules Governing Communications with the Public***. This is significant because FINRA's proposed rule changes will now incorporate **NASD Rules 2210 (Principal Approval) and 2211 (Record Keeping of Sales Material)** and their respective *Interpretive Letters*, while deleting certain provisions of NYSE 472. In essence, these changes will make the rules more streamlined and do not materially affect an organization's obligations to supervise, archive, and to be prepared for discovery regarding content, regardless of the medium in which the content is produced.

In concert, these regulations require that financial companies monitor and archive social media in order to ensure compliance with company policies and various other regulatory requirements for investor protection. These requirements place the onus on the financial companies to maintain the archival/capture of social media websites if they qualify as advertisements or business recommendations. This has resulted in financial companies forging the way many non-regulated companies are headed, toward proactive social media governance and records retention of all customer communication as well as transactional data. Compliance with these regulations cannot effectively be accomplished manually, and requires an archive as well application programming interfaces (APIs). Non-compliance with FINRA's regulations can result in hefty fines for financial institutions; many of these fines are levied due to poor information management, many times social media related.

SOX and Dodd-Frank

The Sarbanes-Oxley (2002) and **Dodd-Frank (2010)** are two federal laws that impact the financial institutions and provide for greater transparency and consumer protection. Social media regulation is not only important to prevent fraud and the dissemination of misleading statements to protect investors, but also imperative as companies must now monitor social media as a duty to their shareholders. The advent of social media has affected valuations of companies in the marketplace due to its quick and viral nature. Investor relations and corporate governance requirements under Dodd-Frank require greater transparency into the real-time monitoring of the social media universe for reporting purposes. The same policies and technologies for monitoring and archiving social media for FINRA compliance also accomplish compliance with investor relations provisions.

Legal Hold

Other laws and compliance considerations exist for organizations that do not yet have codified guidance on social media regulation. As mentioned above, if social media is relevant to litigation, it may be discoverable under the U.S. Federal Rules of Civil Procedure and/or the applicable state law equivalents. It is also important to note that **legal hold** is a requirement in U.S. civil suits that is triggered when there is reasonable anticipation of litigation. Social media, while not widely archived by non-regulated industries, may still be deemed discoverable as the aforementioned cases illustrate.

If an organization elects to archive social media, and if that data is relevant to anticipated litigation, that information is subject to legal hold in the same way any other relevant information to the litigation would be. If an organization chooses not to archive social media, and if content from a social media website is relevant to litigation, they may be scrutinized as to why they did not archive the information and put it on hold if it would have been reasonable to do so. This scenario often arises with a corporate website and marketing material or advertisements; when it becomes necessary to retroactively create what a website looked like at the time of events in dispute.

HIPPA

An example of an industry fast approaching social media regulation is the healthcare industry. The Health Insurance Portability and Accountability Act (HIPPA) of 1996 requires that the identity and any information related to a patient's health be protected as private information. Because of the sensitive nature of medical information; hospitals, healthcare providers and pharmaceutical companies alike would be well-served to mirror the financial industry's stringent guidelines by reaping the rewards that social media has to offer, while managing the risks appropriately. Breaches of patient privacy related to HIPPA may carry severe monetary sanctions as well as imprisonment.

Getting started

The above mentioned requirements, while not exhaustive, certainly provide a framework for what considerations any organization needs to examine to manage social media risks with proactive information governance. Archiving and eDiscovery technologies exist in many organizations today for storage and document retention purposes. Social media is the simply another type of data that needs to be incorporated into the overall information governance plan of an organization.

An archive like EV should be deployed in conjunction with detailed and documented policies, processes and procedures to achieve compliance with the applicable regulatory requirements for managing ESI. Archived information can be rapidly deduplicated, searched, retrieved and deleted to satisfy corporate and regulatory requirements. All organizations must be able to provide defensible documentation regarding the configuration of their IT environment. This documentation must include at a minimum:

- The technologies,
- Policies,
- Processes/procedures governing the environment,
- A person(s) must be designated to defend the solution to a court or regulatory body.

Social media is here to stay. From a discovery standpoint, it is dangerous because it is omniscient, viral, fast, not within the four walls of an organization, and impossible to control without properly deployed technology. The existing information systems within even the most seasoned of litigants will require a rework to control social media and to selectively archive according to specific industry standards and/or business objectives.

It is unrealistic to ban social media use from the workplace, and it is also detrimental from a business perspective to sit on the sidelines and not participate in this vast universe of communication that can yield economic gain. The good news is that the technology exists to address all of the monitoring, archiving and discovery needs of an organization for compliance and litigation. The challenging news is this change is a major paradigm shift for organizations in the way the presently operate. The construction of a social media policy, the integration of that policy into existing document retention practices and the training necessary to implement effective information governance program take a significant time investment; however, many organizations are successfully doing so.

About Symantec:

Symantec is a global leader in providing storage, security and systems management solutions to help consumers and organizations secure and manage their information-driven world.

Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site: www.symantec.com

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934