Creating a Culture of Compliance

Moderator: David Cohen
Panelists: Dawn Radcliffe, Susie Small

Long before litigation arises or a triggering event, organizations can take proactive steps that will lower their risks, create a more defensible process and reduce costs. All of these goals can be achieved by creating a culture of compliance. This is when procedures and policies are in place to anticipate preservation efforts, employees understand ahead of time what their responsibilities are, information management protocols are in force and employees know a trigger event when they see one and know who to alert in the legal department. Some of these efforts can be done reasonably quickly, but culture grows organically through repetition so it is more realistic to consider these to be investments that will take some time to become ingrained at the employee level.

NINE STEPS TO BUILDING A CULTURE OF COMPLIANCE

1. The Importance of C-Level Buy-in

Having high-level buy-in within the company is critically important for setting a tone that these issues are necessary. If it’s just the records department telling people to do things, employees won’t necessarily pay attention. So once you get the executives to buy-in, to implement procedures for retention or legal holds, that all flows down and creates that culture that you need for compliance.

If you have your top people behind the policies, such as the CEO telling everyone that they really need you to do this and here’s why, you’re going to get a higher level of compliance from employees. You’re also going to know that you have the force behind you to do what you want to accomplish.

Educate your company management about why this is important. Your lawyers will also be helpful in communicating this to company management. If necessary, invite outside counsel as a third-party to do presentations at executive meeting about the importance of sound preservation and how, from an electronic discovery perspective, they will save money and reduce liability risks.

2. Adopt Information Management Policies to Limit Retention

One of the best ways to create a culture of compliance is to have fewer records. The fact that electronic storage is becoming cheaper is a dangerous trap. The real cost isn’t the storage, it is those e-discovery expenses that you may be facing down the road when you have kept all that data and now you have to search and process it. Practice good record hygiene. Keep what you need for company business purposes and for legal compliance and for legal holds. Beyond that don’t keep too much.

E-mail is the main culprit since it is the primary system for documenting business communications and for transferring information. Employees tend to hoard data and can accumulate gigabytes and gigabytes of ESI, and are uncomfortable deleting any of it. In trying to change that culture and move toward a better system, it is important to understand the current culture and why people do the things they do, how they access and use the information. Rather than wanting to take everything away from them and inhibiting their workflow, approach them with an understanding of their process and show how a new method will help them by being more organized.

One step is to implement an email archiving which is beneficial because it preserves the data, but in a way that makes it accessible and controllable for purposes of preservation. Moving away from PST files, which are email archives stored on each individual PC and present a huge collection challenge, should be a goal for any organization that has not yet done so.

Also, setting a standard for email retention, be it 30, 45 or 60 days, imposes a clear way to improve data hygiene. However, you have to give employees an alternative for saving emails and other records long-term for legitimate business purposes. If not, employees will skirt the rules and create more headaches.

For example, organizations using Microsoft Outlook Exchange, the leading enterprise email server, one of the easiest ways to do this is to set up folders. Instead of having the folders being on hard drives, however, locate them on shared servers so they are easier to control and collect. This also allows the employee to continue “business as usual” while reducing effort and risk if that information is potentially responsive.

Another major area, and one where we’ve seen significant sanctions ever since the days of Zubulake, are the issue of backup tapes. Most companies keep backup tapes or now sometimes backup information on discs for disaster recovery purposes. But as the IT people in the room can tell you, for disaster recovery you only need the latest versions of what was on your systems. At most, you want to go back days or weeks, not years. There’s no reason for disaster recovery to keep those backup tapes from three, five or 10 years ago. Think about whether you can do backup tape remediation by looking at what backups you have and comparing it with what litigation you have. Usually companies can draw some lines around the litigation and get rid of at least some of the backups.

3. Schedule Records Clean-up Days

Consider having a record cleanup day in which all the employees participate in helping properly store business records and dispose of unneeded files and obsolete information. This effort applies not only to electronic records but to backups and hardcopy archives.

An annual or bi-annual record cleanup day can be organized by records management or legal, and can be used to educate but also try to make it fun, i.e. buy pizza and wear casual clothes. It is an opportunity to clean things out but also to train employees on what a record is. You want employees to get rid of stuff, but also understand what it is that you need to keep.

One final point is to incorporate the idea of a litigation hold into effort. If some records are under a preservation order, then be sure have controls in place to ensure that those are not touched. Again, it is an opportunity to educate about the legal hold process should one be in place and show employees that information can still be culled as long as it is not on hold.

4. Address the Issue of Departing Employees

Many companies get tripped up on the problem of departing employees and it is an issue that needs to be addressed if you have not done so already. It is common to have policies that when an employee leaves, his laptop or office computer is recycled with the hard drive getting wiped. If that individual is a custodian on litigation hold, then that data can be irretrievably lost.

Build a process, perhaps in conjunction with the Legal, Human Resources and Information Technology teams to generate an email alert when an employee is terminated. Legal can check the current list of legal hold custodians to assess whether that computer and other resources that custodian may have are preserved. As a backstop, some companies actually put a sticker or other indicator on computers belonging to employees on legal holds that will prevent IT from mishandling it should they not get word about a departing employee quickly enough.

5. Publish legal hold policies or guidelines and procedures

Give the subject matter of this conference, legal holds are naturally part of the process. This recommendation is specifically referring to publishing to the entire organization written policies and procedures rather than confining them to the in-house legal team. These shouldn’t be the company’s best kept secret! This can be particularly helpful to insulate you from certain sanctions and allegations should spoliation occur.

Anybody that deals with or creates data of any kind needs to understand legal holds and impact on their work. So it is critical to have those policies and procedures out in the wild where everybody can see them and understand them and ask questions about them. Employees appreciate having clear instruction about exactly what they are supposed to do, so having them in writing helps build the culture of compliance right from the start.
Creating a Culture of Compliance

Moderator: David Cohen
Panelists: Dawn Radcliffe, Susie Small

Long before litigation arises or a triggering event, organizations can take proactive steps that will lower their risks, create a more defensible process and reduce costs. All of these goals can be achieved by creating a culture of compliance. This is when procedures and policies are in place to anticipate preservation efforts, employees understand ahead of time what their responsibilities are, information management protocols are in force and employees know a trigger event when they see one and know who to alert in the legal department. Some of these efforts can be done reasonably quickly, but culture grows organically through repetition so it is more realistic to consider these to be investments that will take some time to become ingrained at the employee level.

NINE STEPS TO BUILDING A CULTURE OF COMPLIANCE

1. The Importance of C-Level Buy-in

Having high-level buy-in within the company is critically important for setting a tone that these issues are necessary. If it’s just the records department telling people to do things, employees won’t necessarily pay attention. So once you get the executives to buy-in, to implement procedures for retention or legal holds, that all flows down and creates that culture that you need for compliance.

If you have your top people behind the policies, such as the CEO telling everyone that they really need you to do this and here’s why, you’re going to get a higher level of compliance from employees. You’re also going to know that you have the force behind you to do what you want to accomplish.

Educate your company management about why this is important. Your lawyers will also be helpful in communicating this to company management. If necessary, invite outside counsel as a third-party to do presentations at executive meeting about the importance of sound preservation and how, from an electronic discovery perspective, they will save money and reduce liability risks.

2. Adopt Information Management Policies to Limit Retention

One of the best ways to create a culture of compliance is to have fewer records. The fact that electronic storage is becoming cheaper is a dangerous trap. The real cost isn’t the storage, it is those e-discovery expenses that you may be facing down the road when you have kept all that data and now you have to search and process it. Practice good record hygiene. Keep what you need for company business purposes and for legal compliance and for legal holds. Beyond that don’t keep too much.

E-mail is the main culprit since it is the primary system for documenting business communications and for transferring information. Employees tend to hoard data and can accumulate gigabytes and gigabytes of ESI, and are uncomfortable deleting any of it. It’s important to change that culture and move toward a better system, it is important to understand the current culture and why people do the things they do, how they access and use the information. Rather than wanting to take everything away from them and inhibiting their workflow, approach them with an understanding of their process and show how a new method will help them by being more organized.

One step is to implement an email archiving which is beneficial because it preserves the data, but in a way that makes it accessible and controllable for purposes of preservation. Moving away from PST files, which are email archives stored on each individual PC and present a huge collection challenge, should be a goal for any organization that has not yet done so.

Also, setting a standard for email retention, be it 30, 45 or 60 days, imposes a clear way to improve data hygiene. However, you have to give employees an alternative for saving emails and other records long-term for legitimate business purposes. If not, employees will skirt the rules and create more headaches.

For example, organizations using Microsoft Outlook Exchange, the leading enterprise email server, one of the easiest ways to do this is to set up folders. Instead of having the folders being on hard drives, however, locate them on shared servers so they are easier to control and collect. This allows the employee to continue “business as usual” while reducing effort and risk if that information is potentially responsive.

Another major area, and one where we’ve seen significant sanctions ever since the days of Zubulake, are the issue of backup tapes. Most companies keep backup tapes or now sometimes backup information on discs for disaster recovery purposes. But the IT people in the room can tell you, for disaster recovery you only need the latest versions of what was on your systems. At most, you want to go back days or weeks, not years. There’s no reason for disaster recovery to keep those backup tapes from three, five or 10 years ago. Think about whether you can do backup tape remediation by looking at what backups you have and comparing it with what litigation you have. Usually companies can draw some lines around the litigation and get rid of at least some of the backups.

3. Schedule Records Clean-up Days

Consider having a record cleanup day in which all the employees participate in helping properly store business records and dispose of unused files and obsolete information. This effort applies not only to electronic records but to backups and hardcopy archives.

An annual or bi-annual record cleanup day can be organized by records management or legal, and can be used to educate but also try to make it fun, i.e., buy pizza and wear casual clothes. It is an opportunity to clean things out but also to train employees on what a record is. You want employees to get rid of stuff, but also understand what it is that you need to keep.

One final point is to incorporate the idea of a litigation hold into this effort. If some records are under a preservation order, then be sure have controls in place to ensure that those are not touched. Again, it is an opportunity to educate about the legal hold process should one be in place and show employees that information can still be culled as long as it is not on hold.

4. Address the Issue of Departing Employees

Many companies get tripped up on the problem of departing employees and it is an issue that needs to be addressed if you have not done so already. It is common to have policies that when an employee leaves, his laptop or office computer is recycled with the hard drive getting wiped. If that individual is a custodian on litigation hold, then that data can be irrevocably lost.

Build a process, perhaps in conjunction with the Legal, Human Resources and Information Technology teams to generate an email alert when an employee is terminated. Legal can check the current list of legal hold custodians to assess whether that computer and other resources that custodian may have are preserved. As a backstop, some companies actually put a sticker or other indicator on computers belonging to employees on legal holds that will prevent IT from mismanaging it should they not get word about a departing employee quickly enough.

5. Publish legal hold policies or guidelines and procedures.

Give the subject matter of this conference, legal holds are naturally part of the process. This recommendation is specifically regarding publishing to the entire organization written policies and procedures rather than confining them to the in-house legal team. These shouldn’t be the company’s best kept secret! This can be particularly helpful to insulate you from certain sanctions and allegations should spoliation occur.

Anybody that deals with or creates data of any kind needs to understand legal holds and impact on their work. So it is critical to have those policies and procedures out in the wild where everybody can see them and understand them and ask questions about them. Employees appreciate having clear instruction about exactly what they are supposed to do, so having them in writing helps build the culture of compliance right from the start.
6. Consider maintaining a data map.
A data map essentially lists the different kinds of records throughout the company, shows where they are stored, who controls them and any schedules for automated deletion. In the past, it was in vogue pay consultants six figures to create big, detailed data maps which frankly weren’t very useful because they were too detailed and became outdated quickly.

A “data map” need not be a comprehensive overview of every byte of data throughout an enterprise. It could be a document that lists the top 100 systems and identifies the business and IT owner for each system. When the time comes, it can help the team move quickly to communicate to the appropriate people, in particular where there is ephemeral data that is fragile.

7. Adopt employee training programs.
Education and training to the employee population will dramatically improve compliance when issuing a litigation hold. The lowest impact method is to piggyback on other training efforts and ensure that legal holds have a few slides dedicated to them as part of regular corporate programs – including orientation trainings for new hires. In addition, reinforce the training with some way to certify that the employee has taken the training, or even have them take a short electronic test.

Training and education extends beyond the direct impact of preservation orders, but should also include behaviors. Some examples include how to manage email and purge your inbox of junk. This includes discouraging employees from using their work emails for personal messages. A good way to illustrate this is to imagine that fuss you’re having with your teenage daughter ending up in front of a bunch of attorneys to review it.

8. Prohibit messaging and texting regarding subjects of legal holds.
SMS messages, Skype chats and other messaging tools are becoming more commonplace in work environments. Naturally, this information is discoverable just like everything else. While prohibiting their use is not possible, do try to instill in employees that discussing any matters that are not a part of the audit trail for the litigation hold.

For key custodians, consider going one step further than just having them acknowledge the hold but query them to make sure they are doing what they’ve indicated they would do. When doing this, be sure to record the effort as part of the audit trail for the litigation hold.

Another focus should be on sending periodic reminders to custodians about their ongoing obligation to preserve information, which is one component of the Zubulake opinion. Have a process in place and check that reminders are going out regularly, perhaps once a quarter or more frequently if merited.

If you learn that an employee has not taken the steps necessary to preserve ESI as they had acknowledged they would, be sure to have some disciplinary procedure in place. It can be a serious violation that could materially change the outcome of a case, so having that in place and communicated in advance to employees can increase compliance across the organization.

9. Audit compliance of litigation holds.
It’s one thing to have a legal hold process in place, but another matter entirely to show it is working. Building a feedback loop in the form of an audit process. The first step is to see that custodians are acknowledging their compliance by responding to the litigation hold notice. If the company is using an automated legal hold management system, the legal team can quickly identify those who are not in compliance and take remedial action, either with more frequent reminders, a call or escalation to his manager.

For key custodians, consider going one step further than just having them acknowledge the hold but query them to make sure they are doing what they’ve indicated they would do. When doing this, be sure to record the effort as part of the audit trail for the litigation hold.

Another focus should be on sending periodic reminders to custodians about their ongoing obligation to preserve information, which is one component of the Zubulake opinion. Have a process in place and check that reminders are going out regularly, perhaps once a quarter or more frequently if merited.

If you learn that an employee has not taken the steps necessary to preserve ESI as they had acknowledged they would, be sure to have some disciplinary procedure in place. It can be a serious violation that could materially change the outcome of a case, so having that in place and communicated in advance to employees can increase compliance across the organization.

6 International Issues

Moderator: Hon. Paul Grewal
Panelists: Conor Crowley, Hon. Ronald Hedges

With the fluidity of the global economy, many companies operate in jurisdictions outside of the United States. If a company isn’t facing this issue now, it likely will in the foreseeable future: How do we reconcile our obligations in the United States to preserve ESI with obligations elsewhere to dispose of ESI? There are other obligations than preservation that are important to consider when looking at preservation and production and how to reconcile obligations in the United States with those an organization is subject to in foreign jurisdictions.

The fact of the matter is that it is no longer sufficient to think only of one’s obligations under the Federal Rules of Civil Procedure or similar rules here in the United States. You have to think about what may be required in other jurisdictions where your ESI may “reside.”

HISTORICAL BACKGROUND ON PRIVACY ISSUES

The reality is that the United States’ preservation model has lost the race. The United States has traditionally had a sector-based approach to privacy. In other words, the focus is on specific types of information (such as protected health information) where the risk of misuse has been dealt with by statute.

In 1995, the European Union issued Directive 95/46, which does not set out an EU-wide statute but gives general guidance to, and sets minimum standards for, member countries. Under the Directive, individuals are deemed to have the right to control how their personal identifiable information (PII) is collected, stored, processed, used, manipulated, or transferred. For non-EU countries, if a country follows the minimum standards set forth by the EU, it is put on what is known as the “White List”, meaning the European Union has determined that the country has in place sufficient protection for PII to allow for transfer of the ESI from the EU to that country. Notably, the U.S. is not on that list.

In some countries, citizens have the right to be forgotten. This means that an individual has control over his or her PII and may ask a company that has PII to remove, delete, or make it no longer available.

Another important concept is that privacy regulations are generally triggered by the location of data, not by the citizenship of the data subject. This means that, once the data is in a country, it may be subject to that country’s privacy regime, even if the data is information that relates to somebody who is not a citizen of that country.

PRESERVATION ABROAD

Remember that in the United States the duty to preserve arises when one is aware of litigation or reasonably anticipates litigation. Most countries have no comparable obligation. In the European Union, “processing” is defined so broadly that the mere act of preservation can trigger the Directive and related statutory protections in individual member states. Companies may be faced with conflicting compliance obligations: Preservation may be required here but to do so may run afoul of foreign laws which restrict the ability to preserve or requires affirmative action be taken to delete the information. That is the conundrum for which there is no clear answer.

Due to the disparity in privacy laws, certain situations can arise overseas that are not common in the United States. For example, take the issue of consent: An employee provides “gold-plated” consent on day one, but then leaves the company he worked for and revokes his consent for the preservation, collection or production of his information. “Informed” consent is also vital. You must explain to the employee why information is being collected, what it will be used for, where it will be kept, and who he can contact if there are questions.

If you have been sued or if you reasonably anticipate litigation in the United States and you are now executing on a strategy to preserve data, you have to think immediately about how to square that duty with obligations that may arise in other jurisdictions where the data resides. An important step is understanding how U.S. courts balance the conflicting obligations that an organization may be subject to.