ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Balancing Global Conflict Between Privacy and Preservation Starts with Information Governance

Information Governance

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Connecting the dots.*** Today's digital climate requires that privacy and preservation are bridged, and that both groups are educated on e-discovery, privacy, and the global implications of data deletion and retention. They key to building this bridge is to create a robust information governance system that's customized to the organization.
- ***Preserve and protect.*** It is essential for legal departments to understand that preservation and legal hold initiatives are a legal responsibility of in-house counsel. While involvement of compliance and IT teams is crucial to the success of compliance processes, responsibility for the project should not be inadvertently transferred to other departments.
- ***Balancing act.*** Reconciling data protection and preservation obligations can be addressed through holistic data systems that manage the risks of increasing data volumes throughout the lifecycle, shift away from blanket legal hold, and increase security and privacy measures.
- ***Roadblocks.*** Organizations that have a "save everything" culture will face much greater difficulty in remediating expired legal holds and separating redundant data from what needs to be preserved.

Legal hold and data protection requirements are evolving, and with General Data Protection Regulation (GDPR) implementation on the horizon, new tensions are arising for multinational corporations trying to maintain compliance with both. On one hand, corporations are working to comply in a robust way with US laws to retain certain data for regulatory reasons or as a result of legal hold obligations. On the other, they face strict privacy laws in Europe and other regions compelling them, in some cases, to dispose of data that may contain personally-identifiable information (PII). Courts have demonstrated a firm position when it comes to penalizing parties that fail to fulfill legal hold requirements, issuing spoliation sanctions of millions of dollars in some cases. The pressure to comply with privacy laws is equally intense — for example, earlier this year, the Italian government issued a €5.8 million fine to a UK-based company for its violation of data privacy rules.

These demands live at two opposite ends of the data management spectrum: preservation vs. disposal. However, the tensions between the two are more perception than reality. The execution of simultaneously preserving and destroying certain data can be complementary tasks when strong information governance (IG) designs are in place, and all teams involved are following defined policies across the information lifecycle. The challenge, however, is that organizations (including their legal teams) often don't understand the full picture of the organization's data universe. When an organization is blind to where its data resides and what is in it, it becomes impossible both to meet preservation obligations and comply with GDPR's guidelines to protect and delete sensitive data. By understanding the full scope of the data, counsel can begin to assess the legal requirements involved with it.

Connecting the dots across privacy and preservation

Often, in-house privacy teams are solely focused on the frontend of the data lifecycle, managing data as it is created and entering the organization, but without consideration for the secondary uses or end-life of that data. Privacy teams work independently of preservation efforts that happen on the backend of the lifecycle when data becomes subject to legal needs or must be reviewed and produced for litigation or a regulatory inquiry. Likewise, legal teams working to preserve data typically lack insight as to how data enters the organization or on the privacy limitations that may come into play. Today's climate demands that privacy and preservation programs are bridged, and that both groups are educated on e-discovery, privacy, and the mutual, global implications across data deletion and retention. The key to building these bridges to enable compliance with GDPR and maintain sound legal hold is a robust IG program, tailor-made to the organization's unique profile and multinational presence.

Before examining the steps that can be taken to implement privacy-based defensible data disposal, while ensuring legal hold needs are still met, it is important to understand the societal context and ethical obligations for privacy and legal hold, and how the global stage is evolving around these issues.

Privacy: Laws and ethics

Europe's stance on privacy is rooted in a historical and legal context dating back to WWII, when the German Nazi regime abused documents containing PII throughout Europe. Given this history, Europe has taken a strict attitude in the last several decades toward protecting its citizens' PII and their sensitive personal information (SPI), such as race, religion, and gender specifications. What constitutes PII is defined broadly under the EU Data Protection Directive and includes an individual's name or email address. Institutions doing business in Europe and transferring EU citizens' data

across borders have been long expected to comply with the EU Data Protection Directive, and face sanctions or imprisonment for failing to do so. In Europe, each data protection authority is responsible for the protection of personal information, including the handling of transfers and data breaches. And although they are all working in accordance EU law, each enacts the legislation differently.

Generally, transfer of data outside of the European Union is limited to countries where the protection laws are equal to or stronger than the laws in the European Union, known as “providing an adequate level of protection.” In acknowledgement of this limitation, the EU Commission and US Department of Commerce in 2000 developed Safe Harbor, offering an option for governed transfer of PII from Europe to the United States by certifying corporations that implement certain technical and procedural requirements.

However, two events ultimately rattled the Safe Harbor framework and led to its October 2015 dissolution. The first was in 2013, when Edward Snowden exposed extensive collection of personal communications and other information within the US intelligence community, and it was revealed that EU citizens were included in the scope of what was being used by intelligence agencies. Snowden set the groundwork for a complaint from Max Schrems, who in 2014 brought to the Irish High Court his case against Facebook on the basis that Safe Harbor was not providing adequate privacy protection for EU citizens. The High Court agreed, sending shock waves through organizations that operate across the Atlantic Ocean. Although the EU-US Privacy Shield was developed to replace Safe Harbor, and includes stronger data protection obligations, the new program did not turn the spotlight off privacy concerns in the European Union.

The European Union further strengthened its data privacy requirements in 2016 by adopting GDPR, replacing the Data Protection Directive. Now considered law, the GDPR is being implemented across Europe and full compliance will be enforced beginning in May 2018. This new sweeping regulation requires organizations to meet stringent data protection requirements over personal data of EU citizens and impacts companies that are based outside of Europe. GDPR defines personal data as any information related to an individual, which can include physical address, email address, IP addresses, age, gender, GPS location, health information, search queries, items purchased, and other identifying information.

Clearly, privacy obligations are not going to become any simpler or easier to comply with for global organizations or for those employing EU citizens. Many of the requirements within the GDPR are focused on data that organizations are collecting from outside of the company, such as non-custodial, customer information. An example of this can be taken from the financial services industry, wherein institutions house extensive PII on behalf of customers as well as their employees. In cases where individuals who are no longer customers of a bank wish to exercise their “right to be forgotten,” under GDPR, it can be very difficult for the bank to comply. Most organizations do not have the programs in place that enable them to easily locate and track this type of data and make it accessible to privacy teams that are looking fulfill data disposal requests from customers.

The pressure to preserve

While limited case law around preservation requirements exists in most jurisdictions, in the United States we’ve seen countless matters that inform the judicial expectations to adequately preserve data that is relevant or reasonably expected to become relevant to litigation or regulatory inquiry. Summarized as the following by a recent article from the law firm Paul Hastings, Federal Rules of Civil Procedure (FRCP) 37(e) “authorizes courts to issue sanctions where four conditions are met: (1) the ESI at issue should have been preserved in the anticipation or conduct of litigation; (2) the ESI

is lost; (3) the loss is due to a party's failure to take reasonable steps to preserve it; and (4) the ESI cannot be restored or replaced through additional discovery."

Changes to Rule 37(e) in 2015 were designed to place reasonableness limits on spoliation sanctions, but over the last year, we continue to see varying judicial interpretation for imposing sanctions. For example, in the 2016 ruling in CAT3, *LLC v. Black Lineage, Inc.*, the judge indicated the court's power to order sanctions even if the decision was not directly consistent with the guidelines in Rule 37(e). The monumental ruling and US$8.5 million fine against Qualcomm and a handful of its lawyers in 2008 is another infamous case that draws to mind the potential severity of consequences for spoliation of evidence.

It is critical for legal teams to understand that preservation and legal hold initiatives are a legal responsibility that must be spearheaded by in-house counsel. The involvement of compliance and IT teams is essential for the overall success and process implementation, but legal departments must not transfer responsibility of ownership to other groups. In many cases, the emphasis on creating a partnership across groups can become a scapegoat for the failure to fully execute putting sound preservation policies and procedures in place. This effort involves the legal department making difficult decisions about processes, acting on knowledge about who and what should be placed on legal hold, issuing notices when new preservation obligations arise and tracking companywide compliance with the policies to ensure data under a legal hold is not deleted. It is common in the legal profession to see counsel avoid taking full ownership over these issues and others that are rooted in technology.

Unfortunately, pressures to preserve have led to overcompensation in this arena, with many organizations responding with blanket holds. Particularly in the financial services and pharmaceutical industries, which typically have heavy litigation portfolios, blanket holds are common. A 2014 study from Iron Mountain indicated that nearly 80 percent of organizations cite a keep-everything culture as a key impediment to defensible disposal implementation. The study also found that 68 percent of data that is eligible to be destroyed cannot be readily separated from legal holds at 56 percent of organizations, and more than half of organizations over-preserve information pursuant to legal holds. With this, important electronic data cannot be located and used when needed at 78 percent of organizations. Further, a 2016 report from Cisco noted that the average cost paid for each sensitive lost or stolen record increased six percent from 2015 to 2016. These statistics underscore just some of the negative consequences that result from blanket retention.

Critical to laying the foundation for a new data program is obtaining historical context from a long-term, permanent insider. It can be challenging to secure involvement and resources from an individual or small set of individuals that have this deep level of insight about the company's litigation profile, but the insight is essential. A legacy list of custodians on legal hold, previous, ongoing, and pending or expected litigation and existing policies will inform and guide processes going forward.

Achieving balanced programs

Reconciling data protection and preservation obligations can be addressed through holistic data programs that manage the risks of increasing data volumes throughout the data lifecycle, shift away from blanket legal hold, and increase security and privacy measures. Legal teams that have been in the habit of relying on blanket holds face a mindset shift to achieve smart, defensible disposal. The following outlines key steps counsel can take to begin implementing programs to bring data under control and simultaneously meet privacy and preservation demands.

Leadership buy-in: The first step is a strategic decision made by company leadership that IG is a priority, and that the C-suite has committed to and is invested in the project. Having equal support from leadership within the legal department — someone who works closely with the people that are doing the actual work — is important to help reinforce priorities and communicate the project's overall importance to the department. IG teams may not worry that the general counsel is going to darken their door if the work isn't done, but they are more invested if their boss or their boss's superior is supporting the initiative. This senior level involvement also helps establish roles and responsibilities, define the risk profile, and ensure resource allocation.

With sufficient support among company executives and in the legal department, teams can then develop important alliances across functions to support the initiative. This includes bringing key stakeholders from IT, compliance, security, and records management to drive certain aspects of the work and advise on how the project will impact their responsibilities.

Collecting legacy information: Ensuring that data is properly preserved downstream, particularly in the midst of a defensible disposal exercise, requires that legal possess specific and accurate records regarding the scope of existing legal preservation obligations. The in-depth scoping of cases and the individuals relevant to them, and the tracking of the entire pool of knowledge can be burdensome and time intensive. While outside resources may be able to provide valuable assistance, for a large organization, heavy involvement of an in-house resource with deep historical knowledge of the litigation portfolio may be necessary too. This effort includes remediating old data from blanket legal holds that are no longer needed. Once everything is thoroughly scoped, the legal team can work with IT to dispose of unnecessary data and deploy technology and policies that automate retention and disposal schedules moving forward.

Take a look in the mirror: An organization's ability to implement preservation orders depends on the quality of instructions from legal. Regulatory and litigation requests are often vague and are not couched in terms that correspond to how organizations store documents. For example, all documents, including communications related to transactions with a particular party, can implicate emails sent by an entire business unit and multiple databases where client transactions are stored. Implementation of legal holds in a targeted way requires legal to put in place processes to bridge the language barrier between legal actors and front office functions.

Building bridges between privacy and preservation teams: In addition to the in-house counsel who guides the legacy information compilation, it is equally important to identify a stakeholder who can serve as a bridge between the privacy and preservation programs. As mentioned earlier, counsel on the back-end handling e-discovery must have a way to connect with the front-end privacy teams to gain advice on how data may and may not be used. A cohesive strategy can be developed from those insights. When a sophisticated data management program is in place, these teams are supporting and informing each other and working together when needs for FRCP compliance and privacy laws clash. Each company is unique, and the IG teams must determine the ins and outs, either by opening the lines of communications across teams or by hiring outside providers to come in and evaluate processes.

Common roadblocks

To execute on the steps above and get an effective data program off the ground, legal teams must secure funding, a solid team of people, and new technology. For small companies, it can be difficult

to get preservation and privacy programs off the ground, as the risks may seem remote and the short-term impact of blanket holds may be smaller. Conversely, at a large organization, the business case may be easier to make, but the sheer size of the company can make scoping difficult and requires software tools that can scale. Gaining collaboration from the many groups that need to be involved in the solution and conducting comprehensive scoping across a global organization is tedious. The timeline for completing this work should not be underestimated.

Organizations that currently have a keep-everything culture will face much greater difficulty in remediating expired legal holds and separating redundant and outdated data from that which must be preserved. More sophisticated organizations likely have taken some of the necessary steps to bring data under control, but many find that programs have too many owners to be effective or that ongoing policy enforcement is not in place. When considering privacy in the context of data volumes, it is important to acknowledge and address that sensitive customer data such as credit card information, social security numbers, and other PII is coming into the organization all the time, in a variety of formats, and from a range of sources. This information ends up in structured databases, into which counsel typically has little to no visibility, but is nevertheless responsible for protecting from breach or privacy invasion. Any effort to establish data governance programs must take all of these challenging and complex factors into consideration.

It is inevitable that counsel will continue to see an increasing tension between privacy demands and preservation obligations, and struggle to marry the two in a defensible and sustainable way. Conflicts between counsel in Europe looking to maintain data protection compliance and those in the United States focused on following the letter of the FRCP laws will surely arise in cross-border matters. The ongoing evolution of global policy — with GDPR at the current forefront — must be the lens through which local procedures are regularly reevaluated and refined. With in-house counsel at the helm of a collaborative and global effort, multinational corporations will be much better positioned to sufficiently meet obligations in every region in which they operate.

Enforcing and maintaining IG programs

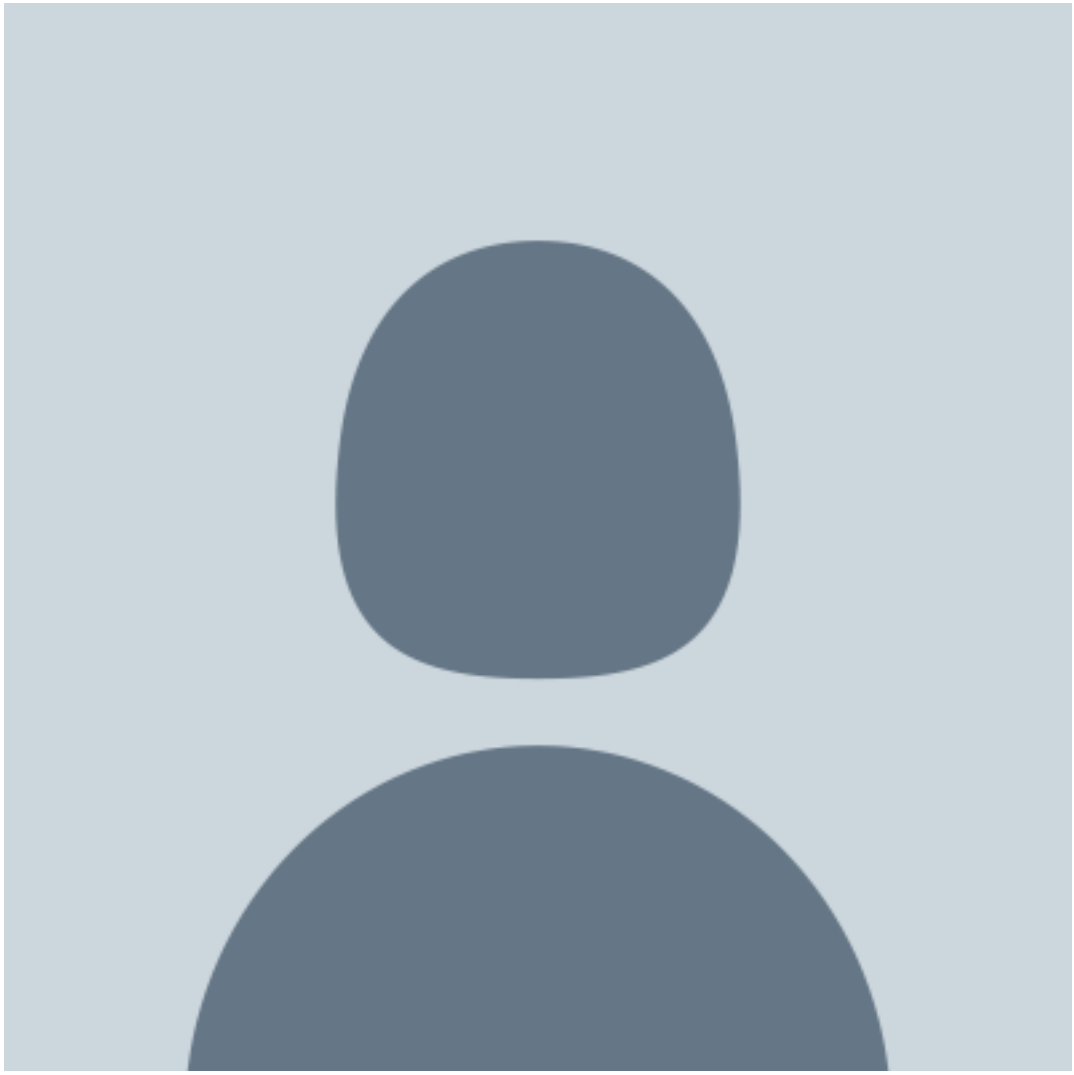
Once a data management program is off the ground, with privacy and preservation teams working collaboratively, it must be well maintained. A sound IG program is only as strong as its enforcement. Ensuring compliance with retention and disposal policies is in and of itself an intensive process, but there are a handful of practices that will help legal teams build long-term success into their overall IG programs. These include:

- **Risk framework:** Allow the company’s tolerance for risk and how programs impact the business to guide decisions about policies, so they are properly aligned and fit into the organization for the long term.
- **Change management:** Examine company culture, incentive programs, and general attitudes towards compliance, privacy, and security; leverage best practices from established change management guidelines such as the Kotter 8-Step Change Model.
- **Training:** Customize training materials that encompass policies and new software tools and make them accessible through a variety of mediums that employees are likely to consume.
- **Work with local counsel:** In cross-border situations, it is important to work closely with local counsel in each jurisdiction to ensure ongoing understanding of and compliance with data protection requirements.
- **Strategic technology selection:** Ensure all key stakeholders are involved in technology evaluations and that deployed solutions offer automated retention schedules and built-in

compliance features.

- **Monitoring:** With the proper tools in place, ongoing compliance monitoring and flagging can take place, notifying the legal team when legal holds are not being followed; tools can also automatically preserve a copy of data that falls under legal hold parameters, even if the user deletes it.

Rachel Marmor



Global e-Discovery Counsel

Barclays

She advises on legal issues related to the use of data in the litigation process, as well as on the management of data throughout the information lifecycle. Marmor was responsible for the establishment of Barclays' in-house e-discovery function and has served as the company's lead e-discovery advisor on high-profile litigations and investigations across the globe.

Jake Frazier

Senior Managing Director

FTI Consulting, based in Houston, TX

He heads the information governance and compliance practice in the technology segment. Frazier assists legal, records, IT, and information security departments identify, develop, evaluate, and implement in-house e-discovery and information governance processes, programs, and solutions.

Ted Barassi

Managing Director

FTI Technology’s Information Governance & Compliance Practice (IG&C)

He brings more than 10 years of experience in the information governance field, and a diverse background spanning the legal, financial services, and software industries. Having practiced law for a decade before moving into technology, Barassi understands the key pain points and legal drivers facing in-house counsel, and combines that understanding with expertise in leveraging software to solve challenges.