COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2021
Increased regulatory scrutiny calls for rigorous data governance

By Bobby Balachandran

Bobby Balachandran (bobby.balachandran@exterro.com) is the founder, president, and CEO of Exterro in Portland, Oregon, USA.

As general counsel and any compliance officer will tell you, COVID-19 has sparked a boom in regulatory scrutiny.[1] There's an incessant flood of internal investigations,[2] employment claims, and corporate audits triggered by pandemic-related workforce reductions, disrupted corporate compliance processes, and dispersed working practices. Added to this are the uncertainties of a slew of new employment regulations; the impact of the California Consumer Privacy Act (CCPA) and its successor, the California Private Records Act; plus the European Union (EU) General Data Protection Regulation (GDPR) directives and a looming federal privacy law for the United States.[3]

Facing these growing compliance burdens, legal teams are of course taking steps to mitigate risk. One of the key strategies to tackle regulatory obligations is building reliable, defensible data management strategies. It's a complex task since organizational data reside in so many different areas with many different data stewards from finance to information technology (IT) to human resources to marketing. Therefore, it is key for legal teams to have the ability to rapidly find and examine data, particularly in response to investigations, litigation, and second requests. Tools, experienced investigators, and forensically sound collection techniques work in harmony to prove that the original data are defensible. This sharpens the focus on data integrity.

Data integrity and defensible data

Each different function in an organization has its own definition of data integrity—enterprise IT thinks about transactional integrity while cybersecurity focuses on the safety of information, and so on. At its core, though, data integrity is an assurance that what was originally created and what people (including investigators) see at a later date remains the same from start to finish. This is the beating heart of defensible data.

The straightest path to data integrity is by instituting processes and workflows that allow information to be collected, searched, and preserved in a consistent fashion. Considering the increasing rate of privacy regulations and compliance mandates related to data security, organizations should take a proactive approach to layer all of the data in a way that is easily searchable and reviewable should a legal issue unfold, such as litigation, second requests, Freedom of Information Act requests, and internal or forensic investigations.

General counsel and compliance officers have to manage an increasingly difficult balancing act between demonstrating governance and compliance, minimizing legal risk, reducing costs, and improving productivity. To help juggle all of this, legal, general counsel, and compliance teams are increasingly turning to single-platform solutions. Why? Varied-point solutions can cost a fortune in time and money, because not only do they have to be managed separately, but there's additional challenge in managing the interplay and incompatibilities between products as they evolve. Therefore, it's far more efficient to use technology platforms that can integrate and orchestrate departmental processes across different workflows, making the data easily defensible and searchable.

The cost of failed compliance and data governance

Firms spend millions of dollars annually on whistleblower hotlines, training, and other efforts to ensure adherence to laws, regulations, and company policies. Yet compliance breaches are common in this legislation-laden landscape due to a mixture of human error, failure to follow up on training, and inadequate organizational metrics.

In 2019, children's apparel firm Hanna Andersson was fined for a breach in the first lawsuit referencing CCPA data management requirements.[4] Another recent example is Doorstep Dispensaree Ltd,[5] a United Kingdom pharmacy, which was penalized in 2020 for poor information governance and records retention after boxes of patient papers were found piled in an exterior courtyard. In the past two years, EU authorities have issued more than €370 million[6] in GDPR fines to small and large organizations, including a $57 million fine for Google,[7] a $123 million fine for Marriott International,[8] and a $230 million fine for British Airways.[9] German web hosting company 1&1 was fined €9.55 million ($10.6 million, later reduced to $1 million) by Germany's Federal Commissioner for Data Protection and Freedom of Information for not taking "sufficient technical and organizational measures" to prevent unauthorized persons using its customer service department to gain access to customer data.[10]

Today, as businesses adjust to coronavirus measures, including remote and distributed working, preemptive data monitoring is essential to ensure compliance and enable corrective action in health and safety, Securities and Exchange Commission compliance, and environmental or ethics matters. Defending data has become a bit more difficult given the prevalence of remote working and the use of collaboration/communication tools to produce far more data than centralized platforms. Data are spread out across locations and devices, making the acts of data collection, processing, and preservation for internal investigations much more complex.

Moreover, the volume of data transfers has greatly increased, opening the door to compromised data integrity through human error as well as deliberate hacking or destruction. Because of this, solutions that can prove and support data integrity will increasingly feature in organizations' strategies as they respond to compliance requests.

The importance of checking for tampering

In investigations, the digital evidence that teams need to review and potentially produce includes a wealth of data from text messages, digital photographs, videos, social media profiles, conversations, emails, and even memes and emojis. Organizations must be able to prove that the evidence produced has at no stage been compromised or tampered with. In unskilled hands, data can negatively alter the course of an investigation, which puts the organization at risk. For example, when trying to preserve email, it can inadvertently be altered, corrupted, or lose critical metadata if not handled properly. This is just one reason why it's prudent to use experienced analysts who use best practices to forensically collect and preserve data.

How do you demonstrate that what is produced as evidence has truly remained the same throughout any business process, including investigation? Having a solution and accompanying process in place that can vet the data for you ensures consistency and reliability, which in turn helps organizations halt errors, improve integrity, update processes, and do all of it defensibly.

Solutions that support healthy data governance and internal investigations should offer the following attributes:

- **Retrievability and accessibility**: The ability to collect data from within and outside the corporate network, cloud data sources, and remote endpoints, as well as the ability to accommodate compliance regulations,

including GDPR.

- **Traceability**: The ability to locate and trace relevant data and link the data back to the source, provide visibility on the traversal cycle, and associate people to it.
- **Reliability**: The ability to produce repeatable and defensible reports on the data when under examination.

Data governance and investigation implications

Effective data governance ensures consistency and transparency and is vital in enabling compliance and legal teams to produce better data analytics—which in turn leads to better decision-making and improved operational support. Further, it helps to avoid data inconsistencies or errors that lead to integrity issues, poor decision-making, and a variety of organizational problems.

If an organization's data are altered or deleted and you have no way of knowing how, when, and by whom, it can have a major impact on data-driven business decisions or the outcome of ongoing litigation. This is another reason for prioritizing data integrity.

The ability to demonstrate data integrity is the cure for many compliance headaches. Further, once the defensibility of the original data has been established, legal teams then have a solid benchmark from which to make continuous improvements to their data governance.Consider these examples:

- Organizations can use forensic investigations to understand, evaluate, and act where privacy protections or other regulatory requirements may be out of compliance and use these data to close loopholes and amend internal practices to ensure they are in compliance with the ever-changing array of global regulations.
- Compliance investigations require that the integrity of the file be validated against evidentiary reference such as the source of the file, access to it, modifications made, where it was transferred to, and via which channels. Once a red flag is detected, compliance and ethics teams should deploy technology that can quickly enable them to investigate all information across all data sources.
- For human resources investigations such as harassment, abuse of corporate assets, or employee misconduct, it's possible to build a complete picture of the true course of events by examining diverse data types such as email exchanges, social media chats, multimedia analysis, or system artifacts. Single-platform technologies enable rapid examination and reporting in all findings.

Looking ahead

During 2021, organizations will be bracing for a further surge of COVID-19–related investigations stemming from liability, employment, and business securities claims. Employment regulations will continue to tighten as states update their responses to the pandemic economy. And we can expect proposals for legislation mandating a comprehensive federal privacy law in response to the current state-by-state regulations. Compliance and ethics teams across all industries will become an even more critical part of ensuring their organization is safe and can grow without spending excessive man-hours and money on regulatory adherence.

Takeaways

- Ensure you have a comprehensive, accurate data inventory. You need to know who owns the data, where the data live, and which regulations govern the data.
- Know which third parties have access to and use your data.

- Ensure you keep only the data you *need*, so that you are in compliance with retention rules, legal holds, or business value.
- Data you don't need should be disposed of, because from a privacy perspective, companies will face higher fines if they don't have a consistent retention/disposition process.
- Build adaptability into your data governance strategy by using solutions that empower you to proactively and defensively maintain the highest level of data integrity.

1 U.S. Securities and Exchange Commission, "SEC Division of Enforcement Publishes Annual Report for Fiscal Year 2020," news release, November 2, 2020, http://bit.ly/2MINXJv.
2 Nicole Hallas, "Class Action Lawsuits and Regulatory Litigation Related to COVID-19," *Audit Analytics* (blog), April 30, 2020, http://bit.ly/30FbmJ3.
3 James Coker, "Will the US Move to a Federal Privacy Law in 2021?" *Infosecurity Magazine*, December 18, 2020, https://bit.ly/3cB0yJu.
4 Amanda Doran, "Hanna Andersson Agrees to Pay $400,000 in First Class-Wide Data Breach Settlement Citing CCPA Statutory Damages," DisputeSoft, January 18, 2021, https://bit.ly/3tohYzi.
5 Jenny L. Holmes, "U.K. data regulator issues first fine under the GDPR," Casetext, January 30, 2020, http://bit.ly/30FMS2h.
6 Jenny O'Brien, "GDPR Fines Hit These Companies Hard. Here's How to Avoid Them." Auth0 (blog), December 30, 2019, http://bit.ly/36XYd7Y.
7 Adam Satariano, "Google Is Fined $57 Million Under Europe's Data Privacy Law," *The New York Times,* January 21, 2019, http://nyti.ms/39HqGk3.
8 Kate O'Flaherty, "Marriott Faces $123 Million Fine For 2018 Mega-Breach," *Forbes*, July 9, 2019, http://bit.ly/3rjPd4Y.
9 Sean Keane, "British Airways faces $230M GDPR fine for 2018 data breach," *CNET*, July 8, 2019, https://cnet.co/39JEJpl.
10 Mathew J. Schwartz, "GDPR Violation: German Privacy Regulator Fines 1&1 Telecom," Bank Info Security, December 10, 2019, http://bit.ly/3rizPFY.