COSMOS
Navigate the Compliance Universe

CEP Magazine - January 2023

Randolph Kahn (rkahn@kahnconsultinginc.com) is Founder & President of Kahn Consulting in Highland Park, Illinois, USA.

Jay Cohen (jcohen@ghclaw.com) is Of Counsel to the law firm of Giordano Halleran & Cielsa and a Senior Advisor at Compliance Systems Legal Group in Wilton, Connecticut, USA.

Data and compliance: A guide to being an information herder, Part 1

By Randolph Kahn, Esq., and Jay Cohen

A recent headline encapsulates the problem big business has with data and compliance: "Large Wall Street firms agreed to pay $1.8 billion in fines over failures to keep electronic records such as text messages between employees on personal mobile phones."[1]

Isn't it strange how little some companies care about one of their most valuable assets? A shipping company knows where every shipping container is located 24/7. A financial institution documents the existence and ownership of every asset in its control. A restaurant chain micromanages its inventory so it has the freshest product for customers with minimal waste and maximal profits. But every business today is also an information business; most big companies spend significant portions of their budget on IT to make their business efficient, competitive, and responsive to their markets and customers. The commodity of information is so valuable that it is sold and traded and has transformed businesses. And yet, most executives have little to no clue about all the information assets their companies have or how they are being created and used. And that is a compliance failure waiting to happen and a strategic advantage squandered.

The ever-evolving information legal environment

With each passing year, more jurisdictions regulate information in more ways, and that doesn't appear to be slowing down. As the information universe expands, so do the laws and regulations that seek to regulate it. It is not just the European Union (EU) and its privacy laws; United States jurisdictions are becoming more prescriptive in how the various states and the federal government expect information to be managed. Increasingly, laws and regulations dictate what your company can and cannot do with information, how long to keep it, how it needs to be secured, and how it must be managed. So, companies are well-served to stay on top of relevant laws and regulations as they evolve and grow.

One such example may make the point. Recently, the U.S. Department of Justice (DOJ) issued a revised memorandum to guide federal prosecutors in evaluating corporate compliance programs.[2] This guidance includes a discussion of the need for corporations to bolster their information management practices relating to new communication technologies and the use of personal devices for work purposes. According to the DOJ, "all corporations with robust compliance programs should have effective policies governing the use of personal devices and third-party messaging platforms for corporate communications, should provide clear training to employees about such policies, and should enforce such policies when violations are identified." So, companies are well served to revisit their policies, practices, retention directives, and training.

Becoming an information herder, not a hoarder

So, what makes an information herder and not a hoarder? It's about right-sizing your information footprint—promoting business and compliance in the process—by knowing what information assets you have, keeping them in conformity with records-retention policies and requirements, and then purging outdated content in the ordinary course of business.

This two-part article is a guide to unearthing information-related issues with compliance, legal, or privacy implications and then developing a plan to better take control of information assets to be more competitive and harvest the economic value of information, while mitigating risk and promoting compliance. Part 1 will describe the various information-related legal and compliance issues, and Part 2 will provide a road map to fix them. In this way, you can help your organization become an information herder, effectively managing your information, rather than an information hoarder, just keeping it all forever.

Information management is a C-suite responsibility

Over time, information has become a clear differentiator. Businesses that use and exploit information properly are rewarded with efficiencies and profitability. Companies that fail to get their information act together wither or sputter. Companies that treat information as overhead and an expense required to run internal operations need to learn how to use that same information as an asset. Legislators and regulators increasingly see information and its management as the responsibility of the senior leaders at a public company. For example, cybersecurity disclosure rules proposed by the U.S. Securities and Exchange Commission (SEC) in March 2022 would require, among other things, that each public company disclose information about its board's oversight of cybersecurity risks and its management's role and expertise in assessing and managing cybersecurity risks and implementing relevant policies and procedures.[3] The rules would further mandate annual reporting about the cybersecurity expertise on the board.

And for some companies, information is the strategic asset that gives their business meaning and value. In such cases, executives understand that protecting, managing, and harvesting information is existential. For example, Airbnb (one of numerous examples) connects consumers and owners of private homes—which is all about information. In essence, the company is nothing more than information and technology.

Today, the mishandling of company information—such as experiencing information security or privacy failure—will mostly likely implicate and impact management like never before. Exposure of company data may be viewed as tantamount to mismanaging company assets, which can negatively impact careers and stock valuations; it may result in penalties imposed by regulators or courts. But perhaps most notably, customers and employees alike expect "their" information to be securely and privately retained; when it gets exposed, the court of public opinion may be the most painful reminder that information matters.