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.

Theft of information and intellectual property

General Keith Alexander, who served as director of the National Security Agency, chief of the Central Security Service, and commander of the United States Cyber Command, once said, "The loss of industrial information and intellectual property through cyber espionage constitutes the 'greatest transfer of wealth in history.'"

And in recent years, the problem of countries, companies, and individuals misappropriating company information and trade secrets of US companies has only become bigger and more expensive to address. Economic espionage is a major drain on competitive advantage, unique intellectual property (IP), and market share. Not only are US companies directly hurt by the theft of their IP, but they may end up competing against their own technology advanced by the IP thief. Protecting this treasure trove of information requires knowing what data

exists, where it exists, who has access to it, and how it is protected.

Growth of information

Information volumes have been growing every year for many decades, and that growth will likely continue unabated. Much of this information is "unstructured"—that is, outside organized databases—and thus difficult to find and organize. Information tends to be ill-managed or not managed at all. Also, companies very often comingle important with unimportant information. That makes environments like the shared drive the perfect target of hackers because employees store all kinds of information there, including data that may have substantial value to the company, like intellectual property, or to its customers, like personal information.

Still suffering from pack rat-itis

Most businesses and their employees keep too much information, and some keep everything. There are various reasons for this reality, which we will explore in Part 2. Suffice it to say, employees usually think all their information is essential, may be of some future value or are afraid to purge content to run afoul of a legal obligation. And at the company level, IT professionals have fallaciously convinced themselves that storage is cheap. When keeping everything is a mode of "management," the law of diminishing returns applies. To the extent that information is somewhere but can't be easily accessed, it is a bad use of company resources. But perhaps more importantly for legal and compliance professionals, that scenario is the worst of all possible worlds. If litigation strikes, it is clear that information is somewhere, but it can't be readily accessed.

The new and ever-expanding universe of information

Companies are challenged not just by the volume of information but also by new technologies, business models, and ways of communicating with employees and customers. There are applications that embed collaboration and communication tools that promote work performance, but these may be less effective at managing the informational output as a company record when necessary. New and more efficient business models put company information in the "care, custody, or control" of third parties, which will be discussed later.

Work from home

Workforces have been gravitating away from the office work setting for the past couple of decades. But COVID-19 was another major game changer for companies and information, though many didn't fully appreciate what was happening to their data gems. As employees were forced to work remotely, they were using technologies to connect and collaborate and store more company information in the cloud and on various home devices with a range of setups and vulnerabilities. We have learned that this reality gives cyber thieves and hackers opportunities to exploit the resulting chinks in the information-security armor. And it creates the obvious issue of how companies will protect, access, and manage information outside their physical control.

Bring your own device, another iteration

The business world has been dealing with employees wanting to use their own phones and computers for work. This has had several iterations, but now it is accepted that companies allow employees to use their own devices for work. The pandemic made this a necessary evil. It makes economic sense for companies to keep employees happier by permitting them to use their own devices, but company information may be comingled on personal devices. The company will need to ensure it has all its information and that its employees protect and follow company rules. Indeed, recent SEC and Financial Industry Regulatory Authority fines totaling over a billion dollars made clear that companies knew their employees were using personal devices and applications to conduct business and had insufficient policies and practices to regulate its use in conformity to law.[4] These fines were

imposed despite the absence of any demonstrated harm to individuals but simply because the firms' compliance programs failed to keep up with and cover their employees' information-management practices.

All companies—not just the broker-dealers and investment advisors sanctioned in these cases—have legal obligations to retain and, at times, produce business-related communications. They would do well to heed the admonition of SEC Chair Gensler when announcing these enforcement actions, "As technology changes, it's even more important that [companies] appropriately conduct their communications about business matters within only official channels, and they must maintain and preserve those communications" as required by law.[5]

Cloud and the explosion of information-storage locations

Most companies are in a new information reality, where more and more information is located in more and more locations that the company may or may not control or own and even may have limited access to. And therein lies part of the problem. Say, for example, the company hires a third-party retirement-plan administrator that manages the information about employee plan participants somewhere in the cloud. Where the information is located, who "owns" it, and under what circumstances the employee or company can access it are all more complicated questions than they used to be. But companies are reluctant to ignore that new reality. More is not merrier when it comes to the proliferation of storage locations. The complexity of understanding where information resides is becoming more challenging with certain types of data, such as smart-device data. Does the data reside on the sensor or device, and does it get transmitted to the manufacturing of the sensor or device? Understanding how data flows and moves is essential in today's world.

To cut costs and have "infinite" scalability, most big companies have moved their data to one of several types of cloud providers or have outside business processes that are not their competency. So, companies like Microsoft, Google, Amazon, or other big cloud-storage providers have more and more of your company's information, and companies are storing less on premises with their own technology.

Third-party providers and contracts

Like the cloud-storage providers, companies are "outsourcing" more company functions to a whole host of companies that provide services and often function through a technology platform owned or controlled by a third-party provider or a contract or provider of theirs. It could be a customer service or human resources company providing human capital management software, or a factor agent providing cash or financing in return for accounts receivable. The critical point is that some third-party company is acting on behalf of another company with storage, control, and/or use of the company's data. Who "owns," retains, manages (and deletes, when requested in some circumstances) that data is rather complex but needs to be addressed.

Likewise, there increasingly are all kinds of relationships that have emerged in the last couple of decades that give some third-party access to other companies' information (usually with consent). Again: who gets to see, use, and manage company information when the company is no longer the holder or controller of that information is a complex question that must get addressed. Additionally, often the wrong company employee is negotiating third-party cloud contracts without sufficient input from other essential stakeholders like legal, compliance, privacy, etc.

Artificial intelligence

Most big companies harness artificial intelligence (AI) daily to answer complex business questions, predict customer needs, respond to customer inquiries, unearth trends, etc. And, of course, AI is dependent on information—usually lots of it. So, employees working on AI projects will want as much information as the company can retain. That, of course, flies in the face of how lawyers, privacy professionals, storage managers,

compliance, and records managers want information to be managed. For them, less information for shorter periods is usually the right answer.

Compounding the complexity of AI data is the reality that not only are volumes a challenge, but when working in the AI space, data is used to unearth answers which may create new and more data. The secondary use of information, as well as what regulations govern it and what privacy consents allow, is a complex problem to understand.

In October 2022, the White House issued guidelines to safeguard personal data in any AI systems and algorithms from misuse in hiring, lending, and other business decisions.[6] Among the five principles in this bill of rights, "to guide the design, use, and deployment of automated systems" is Data Privacy, providing that, "You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used."

Biometric data

Companies increasingly use various biometric data to run their business more effectively and efficiently. Tapping into customer biometric data is part of so many businesses today, including healthcare, medical device, manufacturing, energy transmission, and so many others. That data is arguably owned by an individual who may have given the company access and the right to use the data. And then, there is the question of where the data is stored. Increasingly, biometric data may be stored on a third-party device or server, which the company may not "control."

Internet of Things

The Internet of Things (IoT) is a way in which information is created, collected, and very often sent automatically from one device to another—with or without the device owner's knowledge. For example, say an electric company has installed a smart thermostat that learns family behavior and self-manages the temperature setting for the house without human intervention. Normally there is some ongoing communication between the thermostat, the energy company, and perhaps a third party who made the thermostat or aggregates data for the electric company. But in any event, IoT is a world of connected devices that transmit data through the internet without human intervention. Data grows, but companies don't usually see, touch, or manage it. However, they may still be responsible for it.

Blockchain

Even if you don't think your company is using blockchain, various financial service companies with whom you do business may be. Cryptocurrencies will come and go, but blockchain is here to stay. According to technology-analysis firm Gartner, "Blockchain is a type of distributed ledger in which value-exchange transactions (in bitcoin or other token) are sequentially grouped into blocks. Each block is chained to the previous block and permanently recorded across a peer-to-peer network, using cryptographic trust and assurance mechanisms."[7]

Unlike a traditional clearinghouse, a blockchain implementation does not depend on just one entity to maintain the ledger of transactions. Blockchain relies on many independent third parties—miners—who compete to both verify each transaction and be the first to solve a math problem in exchange for payment. Each miner is responsible for maintaining an independent, often public memorialization of the transaction on the ledger of the chain ("block") of transactions. These miners do not exist in more traditional transactions with banks. Transactions are executed within the blockchain environment and thereafter are aggregated in blocks, which are retained forever and are constantly revalidated with new transactions memorialized in new blocks. The point is that company transactions may be memorialized on a third-party computer without the company's ability to

control such transactions or dictate how long the information related to the transaction is retained.

Digitization

Most large companies are experiencing an acceleration of digitization. That process helps build better business processes through strategic use of technologies. That is significant because it allows companies to reevaluate what they are doing and why. Companies often apply digitization to better-existing business processes without considering compliance needs. In other words, addressing issues such as privacy and security in a project's planning and design phases means it will not need to be retrofitted downstream.

Conclusion

What is clear is that information-related issues for lawyers and compliance professionals are becoming increasingly varied and complex. And those issues are not going away, while new ones appear to pop up regularly. It is no wonder, then, that 79% of lawyers surveyed by Wolters Kluwer for its 2022 Future Ready Lawyer Report said that "coping with the increased volume and complexity of information" is one of the three trends that will have the most impact on the legal profession over the next three years.[8]

Part 2 of the article will demystify many of these issues, provide a roadmap to mitigate risk and exposure, and help your company become not only faster, better, and cheaper but more legally compliant. Gurbir S. Grewal, the director of the SEC's Enforcement Division, made clear the imperative to act now because "a proactive compliance approach" to this new world of information management requires that companies "not wait for an enforcement action to put in place appropriate policies and procedures . . . and anticipate these emerging challenges."[9] To put the task another way, as reinforced by Commissioner Kristin Johnson of the U.S. Commodities Futures Trading Commission on that same matter, "Internal compliance programs must adopt internal controls consistent with this new landscape."[10]

Takeaways

- Companies often do not understand the nature, creation, use, and retention of their information assets, and this is a compliance failure waiting to happen.
- More jurisdictions are regulating information assets in increasingly intrusive ways, so companies must revisit their policies, practices, retention policies, and training.
- The explosive growth in information—much of it unstructured—taxes the ability of organizations to find, organize, protect, and address the risks with these assets.
- Companies are challenged not just by the volume of information but also by new technologies, business models, and ways of communicating internally and externally.
- In-house counsel and compliance professionals must help demystify information management for the C-suite, applying proactive compliance approaches to turn information hoarders into herders.

1 Agence France-Presse, "Large Wall Street firms fined $1.8 bn in US over lax recordkeeping," *MSN*, September 27, 2022, https://www.msn.com/en-ae/money/companies/large-wall-street-firms-fined-1-8-bn-in-us-over-lax-recordkeeping/ar-AA12jIT7.
2 U.S. Department of Justice, Office of the Deputy Attorney General, "Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group," memorandum, September

15, 2022, https://www.justice.gov/opa/speech/file/1535301/download.
3 U.S. Securities and Exchange Commission, "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," news release, March 9, 2022, https://www.sec.gov/news/press-release/2022-39.
4 Agence France-Presse, "Large Wall Street firms fined $1.8 bn."
5 U.S. Securities and Exchange Commission, "SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures," news release, September 22, 2022, https://www.sec.gov/news/press-release/2022-174.
6 The White House, Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, [white paper], October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
7 The DPO Academy, "The Blockchain GDPR Puzzle: An Expert Weighs In," December 6, 2018, https://www.dpoacademy.gr/l/the-blockchain-gdpr-puzzle-an-expert-weighs-in.
8 Wolters Kluwer, *The Wolters Kluwer Future Ready Lawyer*, 2022 survey report, last accessed November 10, 2022, https://images.go.wolterskluwerlr.com/Web/WoltersKluwerLRSUS/%7B60c69227-1c9c-45a1-818f-b7cc4863f1f9%7D_LR_white_paper_2022_09-01_FINAL_single.pdf.
9 U.S. Securities and Exchange Commission, Director of Enforcement Gurbir S. Grewal, "Speech at PLI Broker/Dealer Regulation and Enforcement 2021," (Speech, Washington, DC, October 6, 2021), https://www.sec.gov/news/speech/grewal-pli-broker-dealer-regulation-and-enforcement-100621.
10 U.S. Commodity Futures Trading Commission, Commissioner Kristin N. Johnson, "Statement of Commissioner Kristin N. Johnson Regarding CFTC Orders for $700 Million Penalty Against Bank-Affiliated Entities for Offline Communications," September 27, 2022, https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement092722.