Tech Change Drives New Legal Strategies

June 2018

Bloomberg Law

Big Law Business

Bloomberg Law

Big Law Business

About Big Law Business

Big Law Business is a Bloomberg Law website that provides news, analysis, and information about the legal profession, with a focus on the business of law. Featuring journalists from Bloomberg BNA and Bloomberg News, as well as columnists and contributors who lead and consult the world's largest law firms, corporations and law schools, Big Law Business is focused on the significant developments shaping the legal industry.

The site is designed to provide valuable information and insight to lawyers and professionals who work in big law in the United States, as well as serve as a community for discussion where thought leaders can share their views on cutting-edge trends.

About Our Special Reports

Big Law Business Special Reports are a must-read resource for all business leaders in the legal profession, including in-house counsel, law firm partners, and industry executives. These complimentary deep-dive reports are produced by Bloomberg's Big Law Business editorial team and can be downloadable as PDF files on any device.

Thank you to our sponsors for making this Special Report possible

epiq ankura HighQ

Contents

How Emerging Tech Shapes Litigation

Collaboration Is Changing Custodian-Driven Data Collection 4

Critical Wrinkles of the New European Privacy Law

AI Strategy Needs Close Watching for GDPR Compliance 8

Automation Opens Up Legal, Data Issues

Self-Driving Vehicles Challenge Liability Assessment 12

Impact of SEC Cybersecurity Rules on Companies

New Guidance Stresses Board's Role 16

AI Poses New Ethics Issues for Companies

Who's to Blame When a Robot Makes the Decisions?. 20

How Emerging Tech Shapes Litigation

Collaboration Is Changing Custodian-Driven Data Collection

By Elena Malykhina

Collaborative work environments are becoming the norm worldwide, and the legal industry is no exception. Litigators are using web-based tools to collaborate with others before and after trial, which improves communication and knowledge sharing. At the same time, the number of data locations in collaborative spaces has grown exponentially and has made it challenging to determine the true custody of documents.

When a firm must tighten down the hatches in response to a litigation hold, where does it turn if there are no longer recognized custodians? This scenario is all too real for firms today.

Until recently, a custodian's data was stored on laptops, on personal mobile devices, in desk drawers, in filing cabinets, or even in a personal network space. Now, custodians may have access to dozens, if not hundreds, of data locations, but they may contribute to only a few due to the rise of web-based tools that allow employees to store, access, and share documents. Cloud software is especially popular, with Dropbox, Google Docs, and iCloud named as the top three used by law firms in the American Bar Association's "2017 Legal Technology Survey Report."

"E-mail used to be 80 percent of where the relevant data would reside and still remains a huge part of the equation," said Sean Pike, program vice president of security products at research firm IDC. "But social tools like enterprise instant messengers, collaborative apps, and voice have become a broader part of the custodial focus."

Many e-discovery and archive tools currently on the market have built-in functionality to find, collect, or preserve data across various collaborative apps like Skype for Business and Slack. It's likely that legal holds will target these tools specifically, Pike said.

Despite the benefits, collaboration is decentralizing information, and data gatekeeper roles are disappearing because now employees have access to data they don't actually use, said Joseph Custer, associate professor of law at Case Western Reserve University. This can be problematic when lawyers, paralegals, and other litigation staff need to know who the actual custodians are to produce relevant data.

Social tools "have become a broader part of the custodial focus."

Technology-assisted review can improve the accuracy of document review.

Custer outlined a scenario in which a company, or an unsuspecting representative firm, may put an employee in charge who had access to certain data but no role in the creation, manipulation, monitoring, or even an understanding of the data. "The resultant production of information here could be disastrous," he said.

Growing data volumes are putting more pressure on law firms to use metadata—hidden statistical information generated by a software program—and metadata blast searches to pinpoint the ownership of documents. While some metadata can be useful in placing documents in context, it doesn't necessarily work when document custody must be determined in a collaborative environment.

"Metadata may not tell the whole story or even an accurate story of what documents a custodian truly created, edited, or reviewed," said Andrea D'Ambra, a partner at global law firm Norton Rose Fulbright.

Firms can become more effective at managing data by implementing information governance programs. But even with effective governance policies, the associated metadata may not yield relevant information.

Technology-assisted review is one tool that can improve the accuracy of document review. This algorithm-based process for coding or prioritizing a collection of documents is designed to supplement and enhance an investigation. TAR has gotten to a very efficient level in the past 10 years, although only about one-third of the market has caught on, said Custer of Case Western.

However, technologies like TAR can't solve this problem alone. "Smart firms," as Custer calls them, continue to rely on old-fashioned custodian interviews to find the true ownership of information.

Norton Rose Fulbright is an example of a firm that uses custodian interviews to find the best outcome. The firm typically determines the scope of a custodian's data based on an interview prior to collection. In cases with hundreds of custodians, the firm may send out a questionnaire and then follow up with individual custodians to drill down on ambiguous answers.

There isn't a one-size-fits-all solution, because companies vary in size, the number of custodians they have, and the scope of their collaborative apps, D'Ambra said. Some may start with a metadata-based approach and then seek input from individual custodians.

"Smart firms" rely on old-fashioned custodian interviews to find true ownership.

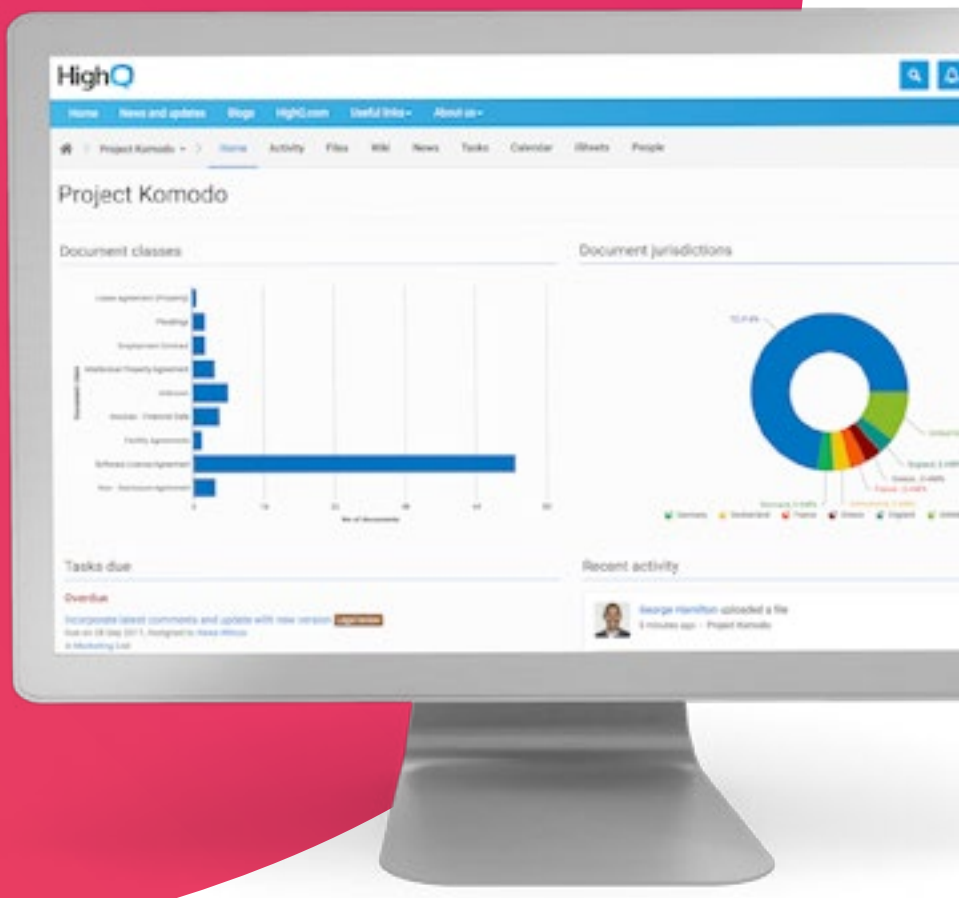
D'Ambra believes custodian-driven data collection will continue to play an important role in e-discovery. Making the litigation e-discovery process more efficient aligns with changes made to the Federal Rules of Civil Procedure in December 2015. One of the changes resolved a historical split among the courts regarding the level of culpability required for a court to issue severe sanctions for failing to preserve electronically stored information.

With the 2015 amendments in place, firms have become more comfortable with engaging in "defensible disposal projects," D'Ambra said. While in the past, firms would vastly over-preserve information in fear of sanctions, now the sanctions are reserved for spoliation done with the intent to deprive the other party of the documents in litigation. Disposal projects can result in significant cost savings for firms, such as reduced storage and review costs for future litigation and data subject access requests.

Reviewing a whole universe of corporate data can be expensive. Getting rid of data unrelated to a litigation and having no value can save trouble and expense later.

Elena Malykhina is a journalist with a focus on information technology.

Are you ready for the future of law?



From culture and relationships to technology, data and processes, the legal sector is changing fast.

Our intelligent work and client engagement platform offers your firm a smarter, safer path forward—transforming your legal service delivery.

A new approach to law starts here. One that's more efficient, transparent and innovative.

HighQ

Visit **highq.com/smartlaw** to learn more.

Critical Wrinkles of the New European Privacy Law

AI Strategy Needs Close Watching for GDPR Compliance

By Lisa Singh

Though the EU's first big data privacy law in 23 years is now in force, there's little consensus on the General Data Protection Regulation. Data experts say GDPR—whose 99 articles govern an individual's right to privacy and ultimate ownership of personal data—is the most complex regulation the EU has ever produced.

The law's brevity may contribute to the lack of consensus. The language of its slim 87 pages leaves a lot of room for interpretation.

This includes both the definition of personal data and a special emphasis where artificial intelligence is concerned. GDPR requires the subject's consent for any evaluation of personal information done solely through the use of AI.

GDPR requires consent for any evaluation of personal data solely through AI.

AI 'Black Box' Versus GDPR Transparency

"There is, on the surface, an inherent tension between the transparency requirements of the GDPR and AI," said industry expert Paul Gettman.

GDPR gives individuals the right to insist that any AI-driven decision—say, on a job evaluation or loan application—be backstopped with human review. That potentially runs counter to what experts call AI's "many opaque and complex decision algorithms" and its "black box" reputation, Gettman said.

By contrast, GDPR requires that data processing be purpose-specific, and that "automated decision-making, including profiling" based on personal data include "meaningful information about the logic involved." That means people will have to be involved. That means people will have to be involved to review use of AI in decision-making.

Yet the essence of AI's power makes this "right of explanation" a challenge.

AI systems' "inherent complexity gives them high flexibility and learning power, [but] also makes it a challenge to interpret the models—or explain the results—produced by them," said Justin Antonipillai, the former acting undersecretary at the Commerce Department who previously helped negotiate the EU-U.S. Privacy Shield.

Data experts differ on whom the GDPR even covers: EU residents, of course, but a U.S. tourist sharing personal data with an AI-driven hotel site in the EU? Prevailing legal opinion says both.

"The GDPR very specifically does not say 'citizen' or 'resident' anywhere" in the 99 articles, said Anne Mitchell, a GDPR compliance attorney. "It says only and repeatedly, 'in the Union.'"

Steep Penalties for Noncompliance

The regulation's expansiveness will challenge businesses to stay clear of penalties for noncompliance: 20 million euros or 4 percent of global annual revenue, whichever is higher. Not all companies are prepared.

"Many U.S. companies without an EU presence but whose websites target EU-based buyers are being caught by surprise that the GDPR expressly considers them within its scope," said Kimberly Verska, a law firm partner and chief information officer who specializes in data privacy and compliance.

Companies, such as HR firms using automated screening for resume submissions, will struggle to "implement consent, human-based review, and regulatory audits where their algorithms and log files are examined for impact on the rights of data subjects," Verska said.

The same holds for companies in health and finance with "aggressive marketing analytics," said Antonipillai, the former Commerce official who's since founded a privacy and security software company.

Staying on the Good Side of GDPR Regulators

Companies that demonstrate good faith in compliance will be well received by regulators—at least initially, experts said.

Verska said that will change as regulators obtain more funding and enforcement resources. Officials have already expressed their willingness to "go after anyone, anywhere," said Mitchell, the compliance attorney.

The GDPR includes a private right of action, allowing individuals to file their own grievances—as Austrian privacy advocate Max Schrems did on GDPR's first day, with an $8.8 billion lawsuit against Google and Facebook.

It will be essential to build transparency into AI systems, experts said. "U.S. businesses that leverage AI-driven technologies for data must be much more transparent about their use, and in some cases must obtain explicit consent before their use," said Bret Cohen, a data and privacy lawyer.

It will be essential to build transparency into AI systems.

Experts also stress the importance of hiring a data privacy officer, although, so far, GDPR mandates this only for companies that process personal data on a "large scale," a term left undefined. In similarly nebulous language, a data protection impact assessment is only required when a technology might trigger "high risk," a category that includes profiling, automated decision-making, and sensitive data collection, Antonipillai said.

Keeping Pace with Unfolding Interpretation

It's not yet clear how and by whom GDPR will be interpreted. The Article 29 Working Party, an EU advisory body that is one of the main groups deciphering the law, has issued guidance on AI-like technologies.

"There are many, however, who disagree about those interpretations, and ultimately, just like here in the U.S., the courts are going to make the final decision," Antonipillai said. "The gold standard is always the courts—the European Court of Justice [and] European Court of Human Rights. The European Commission has real depth on these issues."

The application of GDPR's requirements may ultimately extend beyond the EU, and may be driven by consumer demand rather than government action. There's evidence that some companies are anticipating this. As Facebook's Mark Zuckerberg told reporters in April, "We intend to make all the same controls and settings available everywhere, not just in Europe."

Legal professionals can be expected to play a crucial role in future AI-driven technologies, which will mean incorporating the GDPR privacy mandate by design.

Lawyers "can help the tech industry understand their responsibility when designing systems," said Christopher Byrne, chief executive officer of an EU-based email marketing service. "It's never been more relevant than it is today for GDPR—privacy by design should be on every tech whiteboard."

Lisa Singh is a writer specializing in business and technology matters.

Rise above the challenge with
epiq depth
Powerful solutions that get clients in legal markets around the world from point A to B faster, unless point C is a better option. Expect expert guidance and experience that runs deep with capabilities that reach virtually anywhere.
Learn more at epiqglobal.com
People. Partnership. Performance.
Business Process Solutions | Class Action & Mass Tort | Court Reporting | eDiscovery | Regulatory & Compliance | Restructuring & Bankruptcy

Automation Opens Up Legal, Data Issues

Self-Driving Vehicles Challenge Liability Assessment

By Tam Harbert

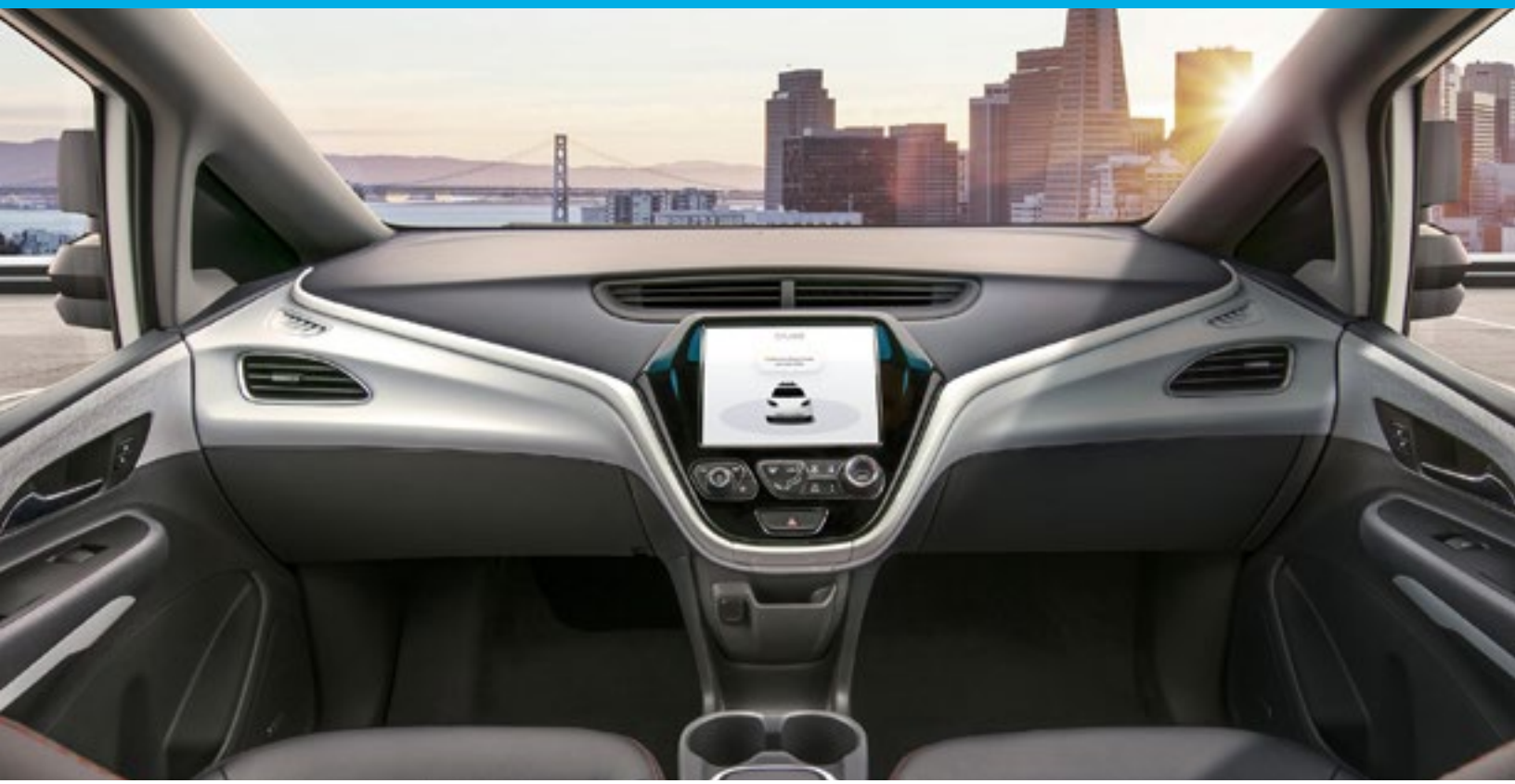
Autonomous vehicles may help make roads safer, but they're likely to raise complex issues in assessing the blame for accidents. Car manufacturers, parts suppliers, and insurers may be looking at a different environment than what they've faced in the past.

Autonomous and semi-autonomous vehicles are touted as a way to make the roads safer. As most accidents are caused by human error, taking control away from the human should mean fewer mistakes, and fewer crashes.

Consumers are skeptical. In a 2017 survey by J.D. Power and law firm Miller Canfield, 46 percent of respondents said they would not ride in a fully autonomous, self-driving vehicle that did not have a human driver's input. Given several recent autonomous vehicle accidents that have made headlines, such skepticism seems justified. In Arizona, an Uber autonomous vehicle hit and killed a pedestrian, and in Mountain View, Calif., a Tesla in autopilot mode crashed into a highway barrier, killing the driver.

Introducing the new technology could make determining liability more complex, as assigning human error will be only one part of the equation. The possibility that cars might make mistakes too adds a new product liability wrinkle to the picture.

Autonomous technology makes determining liability more complex.



Costs for both sides in design defect product liability cases will rise dramatically.

Data Could Be Key in Tesla Crash

The Tesla crash in Mountain View is a good example, said Randy J. Maniloff, an insurance coverage attorney at White and Williams in Philadelphia. In the past, an automaker usually would not be involved in the determination of fault in a single-car accident, except in known product defect cases. In fact, "normally, this is the type of accident that the manufacturer would never even know about," he said.

But if there is a lawsuit—the Tesla owner's family has hired Minami Tamaki to explore legal options—Tesla may have to prove the accident wasn't caused by its technology. "That could be an extremely expensive and time-consuming proposition," Maniloff said.

Tesla has said its autopilot was engaged and gave warnings to the driver before the crash. But Walter Huang, the family's law firm, said its "preliminary review indicates that the navigation system of the Tesla may have misread the lane lines on the roadway, failed to detect the concrete median, failed to brake the car, and drove the car into the median."

More Defendants, Higher Costs

Attorney respondents to the J.D. Power report said they believed costs for both sides in design defect product liability cases will rise dramatically. The increased costs will come from more parties being involved in such suits, which means more discovery, more depositions, and other legal work.

"In autonomous vehicles, [it's often] the suppliers that are developing the source code and algorithms," said Tina Georgieva, senior attorney, product safety group, at Miller Canfield and an author of the report. "What I've heard from the industry is that suppliers won't be handing over that code to the manufacturers because it's proprietary." That means the suppliers will have to be brought in as defendants.

And the lack of design standards for autonomous cars leaves more leeway in disputes. Because of intense competition, many manufacturers use their own, or a supplier's, proprietary design, Georgieva said. That makes them easy prey in plaintiff design defect claims. Because "the automated vehicles may not handle the same environmental situations in the same way," it would be easy for plaintiff's attorney to claim that a different manufacturer's system would have prevented the accident, thus the design of the manufacturer targeted by the lawsuit was defective, she said.

Nevertheless, Georgieva said data from autonomous vehicles could help resolve liability disputes. In the Uber accident, for example, the car's data helped reconstruct what happened, and presumably figured in determining the legal settlement with the victim's family, she said. (The amount of the settlement was not publicly disclosed.)

"Sharing that data could be very helpful in resolving liability much more quickly and cost-efficiently," Georgieva said. "If you can get the data and see what happened, there might be no need for a lawsuit."

But Maniloff noted that the parties in the Tesla crash are drawing different conclusions from the data. The data from vehicles might just add more time and expense as the parties challenge each other's experts and their interpretation of what the data means.

These complications could also raise the cost of insurance for manufacturers because most liability policies don't cover defense costs, Maniloff said. Today, "the insurance company might [cover the manufacturer] for $1 million, which under most policies means the insurer is on the hook for $1 million in claims plus infinite defense costs," he said.

"Manufacturers might ultimately win these cases, but at what cost? Insurers of carmakers and their suppliers are going to be looking at serious cost exposure in these cases."

Tam Harbert is an independent journalist specializing in technology, business, and public policy.

Data from autonomous vehicles could help resolve liability disputes.

Automating the Legal Department

Start with Foundational Steps for Success

Automation drives new risks and proven rewards across industries, why not in the legal industry? Consider the following steps to introduce an automation strategy in your company.

1. FIND YOUR CHAMPIONS

Certain executives understand the application of automation in legal work. Find the people who will provide resources to ensure success, and get them to buy in to the cause.

2. TELL THE RESULTS STORY

Efficiency, cost savings, better use of talent. Tell people how automation can be used to drive ROI.

3. EXPAND YOUR TALENT

Your company will expect you and your team to understand technology and the results it produces. Expand the scope of your hiring practices to include tech-savvy counsel.

Curious? Read more about the use of technology and automation in the legal industry here.

ankura

Impact of SEC Cybersecurity Rules on Companies

New Guidance Stresses Board's Role

By N. Peter Rasmussen

In February 2018, the SEC voted unanimously to issue guidance on cybersecurity risks and incidents. The commission statement builds on and expands the staff guidance issued in 2011, but there are key differences between the two documents.

First, the 2018 guidance comes from the commission rather than the staff. The new advice also emphasizes the role of a company's board in maintaining comprehensive cybersecurity risk policies and procedures that are integral to the disclosure process.

The SEC's cybersecurity guidance is not rulemaking. The release is largely a series of reminders and suggestions about what companies should have been doing all along. The question now, though, is how public companies should prepare to deal with these disclosure issues in practice.

This is particularly relevant in light of the $35 million Yahoo settlement resulting from the company's failure to disclose a massive data breach. Although two commissioners were among those who wanted the SEC to take stronger action, the guidance—coupled with the Yahoo charges and settlement—indicates that the agency is engaged with cybersecurity issues.

Companies should review and refresh their cybersecurity disclosures.

There is no single, standard response to the disclosure guidance.

Disclosure Obligations

Companies must disclose cyber risks and incidents in their annual Form 10-K filings in several places, including risk factors, management's discussion and analysis, legal proceedings, and disclosure controls. LaDawn Naegle, securities lawyer and managing partner of the Washington, D.C., office of Bryan Cave Leighton Paisner, told Bloomberg Law that many public companies are reviewing and refreshing their cybersecurity disclosures in light of the SEC's guidance.

Mindful of the SEC's admonishment to avoid boilerplate, she said companies are considering how cyber threats, security measures, and possible incidents could affect their businesses and reputations. She cautioned that because each company faces a unique risk profile, there is no single, standard response to the disclosure guidance. Each company must tailor its disclosures to reflect its situation.

Naegle noted that companies should be prepared to discuss the impact of both cyber incidents and risks in their business description, risk factors, and possibly management discussion, and to include the costs of cyber incidents in their financial statements, such as remedial measures, revenue losses, product recalls, and any asset impairment.

Board Matters

Under Item 407(h) of Regulation S-K, companies must disclose the extent of the board's role in the company's risk oversight process. The SEC's guidance stressed the disclosure of directors' role in risk management of cybersecurity.

Naegle suggested the commission's emphasis on Item 407(h) may be a backdoor attempt to impose substantive corporate governance requirements on company boards related to cybersecurity risk management.

As stated by the SEC, if "cybersecurity risks are material to a company's business," the 407(h) disclosure "should include the nature of the board's role in overseeing the management of that risk." In other words, a company can't disclose a board's role in cybersecurity risk management if the board does not play such a role and engage with management in this area.

A key takeaway for board members is that they should be actively engaged on cybersecurity matters. The board cannot simply rely on blanket assertions from management that things are under control. Companies may also want to undertake a board education program, and may wish to consider recruiting board members who are conversant with the impact of data and technology on the business and legal environment. Cybersecurity is clearly now a board concern, not merely a matter for the tech department.

Board members should be actively engaged on cybersecurity matters.

Potential Pitfalls

The guidance may highlight possible exposure for chief executives and chief financial officers in their quarterly certifications. While the SEC has not acted in the area, there may be a risk posed by the certification requirements for periodic reports resulting from inadequate information flow. SEC rules require the CEO and CFO to make certifications regarding the design and effectiveness of disclosure controls and procedures.

The SEC specified in the cyber guidance that the certifications "should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact" on disclosure.

If the company's controls and procedures failed to ensure that information about a cyber incident was properly raised for timely disclosure, but the certifications were still made, the company and its CEO and CFO could be at risk for enforcement action.

A Caution

While it is true that the SEC imposed no new formal requirements in issuing its cyber guidance, it is fair to say that all companies should take a fresh look at their cybersecurity and disclosure protocols. In the event of a cyber event, companies must carefully consider their disclosure obligations, initially and as information is gathered and post-incident follow-up occurs. It is clear that "a response of 'we're still investigating' will not be sufficient to avoid material incident disclosures," Naegle said. The Yahoo settlement suggests 35 million reasons to get the answer right.

N. Peter Rasmussen is a senior legal editor with Bloomberg Law, concentrating on corporate transactions and federal securities law.

Bloomberg Law®

Go on. Break the speed limit.

Faster, more effective court opinion research on Bloomberg Law®

Time is money. That's why Bloomberg Law created **Points of Law**. Using state-of-the-art technology, **Points of Law** speeds up case law research, allowing you to quickly find language critical to a court's reasoning, even when buried deep in the text.

Shortened Research Time

You'll navigate seamlessly from a court opinion to the essential language of a court's holding.

Comprehensive Database

Our collection of court opinions is updated daily and features 13 million opinions.

Data Visualization

Using our Citation Map, view most cited cases, relationships among key cases, and changes over time for the point of law at issue.

Continuous Innovation

With Bloomberg Law, you'll enjoy continually enriched content and functionality at no additional cost.

AALL YOUR LEGAL KNOWLEDGE NETWORK™

2018 NEW PRODUCT AWARD
Bloomberg Law
Points of Law

Learn more at bna.com/points-of-law-lp

AI Poses New Ethics Issues for Companies

Who's to Blame When a Robot Makes the Decisions?

By Ellen Sheng

As it gets smarter, artificial intelligence is performing more complex tasks. Whether it's diagnosing and recommending treatment for a medical condition, identifying and executing investments, or evaluating a loan application, AI's growing capability raises legal and ethical issues of having machines, rather than people, make decisions. Who is responsible when a decision goes awry?

Part of the difficulty of answering that question stems from the fact that the internal logic used by machine learning—a segment of artificial intelligence—can be opaque or difficult to explain. Despite what the terminology suggests, machine learning does not replicate human intelligence.

Consider the incident last year when Facebook's AI Research Lab described using machine learning to train two robots at deal-making. At one point, the robots deviated from human language to devise their own for negotiating. Such developments raise concerns about accountability and hidden biases, as well as liability.

The use of automation for a widening range of functions is creating some interesting challenges for lawyers when establishing liability and accountability. A sizable gap remains when it comes to assigning responsibility for decisions made and actions taken by artificial intelligence.

"Historic models we have been looking at for liability are up for grabs," said Michael Sinclair, an attorney with Norton Rose Fulbright, a global law firm.

Massive personal data input and AI processing AI create legal and ethical quandaries.

Framing the Issue

The unintended consequences of artificial intelligence can be framed in two ways. There's accountability, which focuses on what is done during the design phase. Then there's liability.

Much of the focus around the ethics and regulation of artificial intelligence centers on accountability.

"There is always going to be something that will go wrong," said Martin Abrams, executive director and chief strategist of the Information and Accountability Foundation, based in Texas. One way to limit these unintended consequences is a concept referred to as stakeholder-focused stewardship, he said.

"AI has a very disruptive effect on traditional liability allocations."

"It's not about data but the issues around people," Abrams said. There's now more discussion about the ethics of artificial intelligence in part because more observational data is being used and the processing has become more automated. The intersection of massive personal data input and processing by artificial intelligence creates several legal and ethical quandaries.

One example might be cars with smart braking technology. Self-driving cars may be on the horizon, but meanwhile, auto makers are installing increasingly sophisticated systems that monitor driver behavior and the road. Smart braking technology anticipates when a driver will apply the brakes and road conditions.

These are all considered observational data points. When aging drivers who are slowly becoming less observant on the road start scoring lower on attention span, should a smart vehicle report this kind of observational data to the DMV?

Another example might be a smartphone app that tracks numerous observational data points such as location, movement, number of emails written a day, and so forth. Organizations are then able to assess what users are doing, but the accuracy of the assessment may be questionable.

An app called Ginger.io asks questions and tracks numerous data points to evaluate mental health-related behavior. If a user reports being highly depressed, but the collected smartphone data shows the person has been very active during the day, it would run counter to the reported mental state.

"Organizations need to have a process to assess what companies are doing with the data is ethically sound, not just compliant with the law," Abrams said.

In the Ginger.io example, "observational" data needs to be kept secure and private. Keeping personal data secure can be more difficult than anticipated.

"Machine learning, when exposed to training data, creates correlations using the data. This means that it becomes hard to separate the data from the system," said Sinclair of Norton Rose Fulbright. "This is a big issue for companies wanting to license in data to train AI systems."

Also, under Europe's General Data Privacy Regulation, if it has been offered to European citizens, the "logic" used to make a decision must be explainable to the user.

Liability is the other aspect that must be considered. Artificial intelligence makes figuring out who is at fault much more complicated.

"With a driverless car, if there is an accident (in the absence of mechanical fault) the question of liability gets pushed up the supply chain away from the driver. Is it the business that designed the AI system, the programmer, the business that provided the training data or the training, the manufacturer of the car or the retailer who will be liable?" Sinclair said. "Such issues demonstrate that AI has a very disruptive effect on traditional liability allocations."

Commercial Interests

AI also raises the issue of intellectual property rights. If artificial intelligence can autonomously generate data and create works, Sinclair said, what are the IP rights in those situations?

Many intellectual property rights laws around the world require a human creator, or at least a sufficient connection with a human. So regulators will need to figure out how to deal with AI-created works in the near future. There's also a flip side: What happens if AI autonomously does something or creates a work that infringes the IP rights of a third party? Who would be liable in such a situation?

These are questions that legal experts and regulators are examining, and there are no answers yet. AI is developing rapidly, and companies, eager to use AI to their advantage, are seeking ways to achieve legal and ethical compliance. That path will be complicated, with mistakes along the way.

"If you're ever afraid of making a decision because something might go wrong, then you'll never make progress," Abrams said.

Ellen Sheng is a writer and editor with a focus on business finance, fintech, and U.S.-Asia investments.

AI also raises the issue of intellectual property rights.

Bloomberg Law

Big Law Business

© 2018 The Bureau of National Affairs, Inc. 0218–JO25280