Business Adjusts to Data and Privacy Rules

April 2019

Bloomberg Law®

Bloomberg Law®

Bloomberg Law Special Reports

This issue of the Bloomberg Law Special Reports offers the latest insights on trends affecting the legal profession this year. We look at key sectors where data privacy laws are forcing changes, and the coming impact on business and law practice.

Join us on May 14 for our Special Report webinar, How Companies Can Address Emerging Compliance Risks in Privacy.

About Bloomberg Law

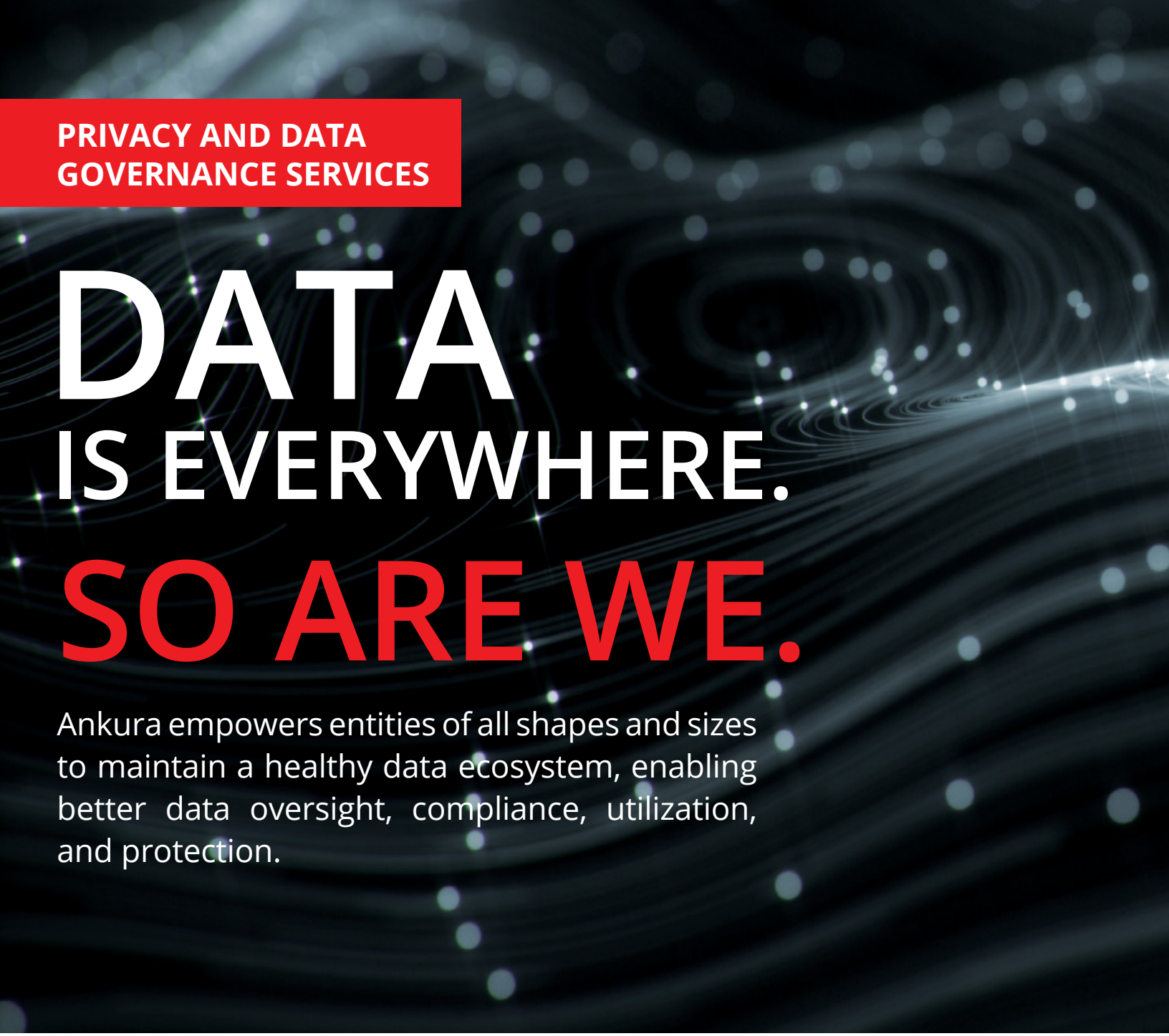
Bloomberg Law® helps legal professionals provide expert counsel with access to action-oriented legal intelligence in a business context. Bloomberg Law delivers a unique combination of Practical Guidance, comprehensive primary and secondary source material, news, timesaving practice tools, market data, and business intelligence.

For more information, visit www.bna.com/bloomberglaw.

Thank you to our sponsors for making this report possible.

ankura integreon mindcrest®

Contents



PRIVACY AND DATA GOVERNANCE SERVICES

DATA IS EVERYWHERE.

SO ARE WE.

Ankura empowers entities of all shapes and sizes to maintain a healthy data ecosystem, enabling better data oversight, compliance, utilization, and protection.

HOW WE HELP

- Privacy modernization programs
  - General Data Protection Regulation
  - California Consumer Privacy Act
- Data mapping and classification
- Records retention and data minimization
- Interim data protection officer and interim CISO services
- Cyber due diligence

ankura.com

ankura™

GDPR Rollout Snags Companies and Regulators

By Ellen Sheng

Businesses and law firms in the U.S. and regulators in Europe are still adjusting to privacy and data protection requirements imposed by the General Data Protection Regulation, almost a year after the law went into effect. GDPR's influence goes beyond corporate action; the European regulation has prompted U.S. lawmakers to introduce varying state laws that could complicate the issue further.

The transition has not been entirely smooth. Large multinationals that invested heavily in data security and GDPR preparation are in management mode, waiting for advisory opinions from regulators. Other organizations are in the middle of making changes to adapt to GDPR. Still others have done nothing, either unaware of the potential impact on their business or too caught up in the day-to-day to embark on a costly data privacy project.

European regulators have blocked more than 1,000 U.S. websites that are not compliant. Even large companies that spent months preparing have been caught flat-footed. French regulators fined Google $57 million for noncompliance, making it the first U.S. tech company to be fined under GDPR. Google has said it is appealing.

The number of data subject access requests has surprised companies.

Companies aren't the only ones still adjusting to GDPR. Regulators are finding they also have to ramp up staffing. Companies and regulators alike are working through GDPR and its implications.

"We've heard many times at our conferences now that GDPR is a journey, not a destination," said Trevor Hughes, chief executive of the International Association of Privacy Professionals. "You shouldn't expect that there's ever a day when you get to clap your hands and say we're done, because that's probably not the case."

One turn of events that's taken companies by surprise has been the sheer number of data subject access requests. Under GDPR, consumers can ask for their data, and organizations are supposed to respond in a timely manner. This has tested companies' technical ability to find the data, which involves a bit of data forensics, and then respond to the individual.

Companies are struggling to meet the demand. U.S. consumers have similar data access rights – such as through HIPAA – but haven't exercised those often. "I don't know if that built a baseline of expectations, but your history is relevant to how you think about the future," said Kirk Nahra, a partner at WilmerHale and co-chair of the firm's cybersecurity and privacy practice.

Another surprise has been the number of breach reports filed. Under GDPR rules, companies that see any kind of data breach need to file a report to the government within 72 hours.

Hughes describes this, too, as a work in progress. "So many organizations are still working through exactly what their regulator of record, or lead authority, expects with regards to notice of security breach under GDPR," he said, adding that 72 hours is a tight deadline to assess what has occurred.

As a result, companies are filing many inconclusive reports. European regulators have been overwhelmed by the number of breach reports, and many have been adding staff and functions.

"There has been enormous activity in the marketplace, but there's still lots more to do," Hughes said.

A 2018 survey by IAPP of its members found that fewer than 50 percent of respondents are "fully compliant" with GDPR and nearly one in five say full compliance is impossible. Hughes said it's likely that the 50 percent figure is on the high side overall because IAPP is an organization made up of privacy professionals, which would exclude companies that don't have any.

Data privacy professionals are busy as companies adjust to GDPR. Many U.S companies didn't even begin compliance efforts until after GDPR went into effect, and many smaller companies are just now figuring out whether and how they are subject to regulations.

Spurred by GDPR, states are also introducing data privacy laws, most notably in California. The state's Consumer Privacy Act, which was signed into law in June, goes into effect next year and will affect how for-profit companies process personal information about California residents and do business in the state. Following in California's footsteps, the Washington state Senate passed the Washington Privacy Act in March. The bill is up for a vote in the House.

GDPR is keeping data privacy professionals busier than ever, according to Bloomberg Law.

This state-by-state approach is creating headaches for U.S. companies, which are facing different standards. Companies including Apple, Cisco, and Microsoft are pushing for more cohesive, nationwide rules about data privacy. In November, Intel floated a federal data privacy bill that is currently open for review and comment from data privacy experts and the public.

"There are companies who are more U.S.-centric who don't want any national law. There are companies who want one law," Nahra of WilmerHale said. "It's all over the map at this point."

For companies that have built out a process to deal with GDPR, proposed domestic regulations complicate matters, because there is not a lot of overlap. While GDPR details what companies can't do and creates principles, California's law focuses on individual rights.

"They don't quite fit together," Nahra said. As a result, companies are struggling to figure out how to approach the potential patchwork of laws and evaluating whether they can apply the process they've built for GDPR in other places. That applies for California's new law, too.

Are companies "going to operate with one principle or … are we going to treat California differently than how we act everywhere else? That's very much an open question at this point," Nahra said. "Every company's going to make their own decision on that."

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


mindcrest®
we're turning
innovative ideas
into actionable
legal solutions
Chicago | London | New York | Pune
info@mindcrest.com
mindcrest.com

Biometric Data Privacy Lawsuits on the Rise

By Tam Harbert

A recent Illinois Supreme Court decision shone a spotlight on biometrics privacy, helping to prompt a wave of lawsuits in that state and leading others to consider similar laws.

The law has opened the door to more cases against companies, according to Bloomberg Law.

Illinois was the first state to enact a law governing privacy of biometric data, including fingerprints, retinal scans, and facial recognition. Its Biometric Information Privacy Act of 2008 requires written notice to and consent from individuals when an organization collects and stores their biometric information, and it limits use of such data. Texas and Washington have similar laws, but Illinois is the only state that grants aggrieved parties a private right of action.

In the case before the court, *Rosenbach v. Six Flags Entertainment Corp.*, a woman complained that an amusement park scanned her 14-year-old son's thumbprint – used for admission into the park – without her consent. In a unanimous ruling, the high court reversed an appeals court decision, saying that a violation of the notice and consent provisions alone, without proof of actual harm, was enough for a person to be an "aggrieved party" under BIPA. The ruling opens the way for BIPA lawsuits to proceed.

It also has spurred an increase in new lawsuits. As of March 14, some 220 cases had been filed, more than 50 of them since the high court's Jan. 25 ruling, said Justin O. Kay, partner at Drinker Biddle & Reath and vice chair of the firm's class actions team. And while the first wave of suits focused on large, well-known companies, smaller companies now are being sued.

"These small companies just are not aware" of the law, Kay said. "They probably don't have the legal budget or even significant legal counsel to deal with something like this."

New legislative proposals on biometric privacy have emerged at both the state and federal level. Just a few weeks after the ruling, a state senator in Florida introduced a bill that was identical to BIPA, including a private right of action, said Al Saikali, chair of the privacy and data security practice at Shook, Hardy & Bacon, which represents defendants in 30 BIPA lawsuits.

In Congress last month, two senators introduced a bill to create a national Commercial Facial Recognition Privacy Act, which would require companies to obtain consent before collecting a person's facial data and would limit sharing of such data.

Although the Illinois ruling tossed aside one argument defendants made to dismiss the case, there are several other valid arguments available, said lawyers representing companies.

One is that finger-scanning systems don't use biometrics as defined by BIPA. The majority of BIPA lawsuits are based on an employer's use of finger-scanning technology to track employee work hours. Such systems help prevent "buddy clocking," in which one employee punches in for another employee.

Melissa Siebert, a partner at Shook, Hardy & Bacon, said such systems don't collect or store actual fingerprints, and so they don't deal with biometric information. Rather, the systems measure small points on a fingertip and use an algorithm to create a numerical representation of the finger to identify the employee, she said.

Another is what constitutes consent. Defendants could argue that by voluntarily using the time-clocking system, employees consented to the scanning and storage of their information. The facts of these cases are "very different from the Rosenbach case," Siebert said. "These are consenting adults clocking in and out to get paid."

Most employers use a system supplied by a third party, whose product collects and stores that data, raising the question of which entity is responsible for any BIPA violation. Some cases have named just the employer; others have named both the employer and the vendor.

BIPA does not specifically set a statute of limitations, leaving an opening to argue for a reasonable limit, Kay said. "Defense would argue it should be short, perhaps as short as a year."

Definitions on the type of violations and limits on the number need to be determined.

Even if a court rules that BIPA was violated, definitions of the type of violation and any limits on the number of violations will need to be determined. BIPA carries fines of $1,000 per "negligent" violation and $5,000 per "willful, reckless" violation, but neither is clearly defined, Saikali said.

"Plaintiffs right now are trying to argue that 'violation' means every single time a person put their finger on the device," he said. Assuming that's at least twice every workday, multiplied by the number of days and the number of employees, that could add up to a massive liability for employers. "I think this is going to be the next wave of litigation under BIPA."

Meanwhile, another state law dealing with biometrics could bring a fresh round of litigation. California's Consumer Privacy Act, which goes into effect in January 2020, is similar to BIPA in that it covers biometrics and creates a private right of action with statutory damages, Saikali said.

"I anticipate there will be a lot of litigation in California," he said, "that will look a lot like the litigation we're seeing in Illinois."

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

When a data breach occurs, and it will...

how will you respond?

Your response needs to be quick, thorough and complete to ensure your risk is mitigated and your obligations are met.

- Global resources on 4 continents
- Rapid response to meet critical regulatory obligations
- Identification & extraction of sensitive personal data
- Preparation of notifications
- Quality-controlled data handling throughout every step
- Increased efficiency through technology enabled workflows

Integreon is a global leader in alternative legal, business and research support services for law firms, corporations, financial institutions and professional services firms.

Contact info@integreon.com for more information on our data breach services

www.integreon.com

integreon

Smart solutions to process driven needs

Informed Consent Will Be Key Privacy Issue

By Lisa Singh

The largest regulatory fine leveled against a company since the General Data Protection Regulation was enacted in May 2018 is poised to reshape business compliance practices across industries.

In late January, CNIL fined Google nearly $57 million, citing what the French data-protection regulator saw as failure to meet the core requirements of informed consent under GDPR. As Google appeals the decision, as confirmed by a company spokesperson to Bloomberg Law, the debate is far from settled about what constitutes informed consent in personal data collection.

"The notion of informed consent is essential to the success of any privacy regime," said Elizabeth Banker, vice president and associate general counsel at the Internet Association. "However, CNIL's opinion doubles down on a consent model that may result in over-notification of consumers without delivering better privacy protections."

A pre-ticked box requiring no affirmative user action was ruled invalid consent, according to Bloomberg Law.

Google maintained that its pre-ticked "I agree" boxes sufficiently covered user agreement across the myriad data processing activities that underpin advertising personalization. CNIL, however, held that the notification failed to follow the "essential principles" of consent – freely given, specific, informed, and unambiguous.

The ruling holds far-reaching implications for companies whose revenue is driven by personalized ads. In reassessing online behavioral advertising practices, experts said, companies face a conundrum.

"On the one hand, they are being told their policies must be clear and concise," said Daniel Castro, vice president of the Information Technology and Innovation Foundation. "On the other hand, they are being told their policies must be complete and comprehensive."

Given the balance of obtaining valid consent and complying with the right of consumers to withdraw agreement at any time, legal experts advise sidestepping the need for informed consent wherever possible.

"The key lessons from the decision are, first and foremost, that consent is a high-risk lawful ground to process personal data and should only be used [as] a last resort where no other lawful ground is available," said Ross McKean, partner in DLA Piper's London office and co-chair of the firm's data protection practice.

McKean cites the GDPR's inclusion of various "other lawful grounds" for gathering personal data, such as where processing is necessary for performing or entering into a contract, or where processing is in the legitimate interests of the controller, or a third party – "provided these are not overridden by the rights and freedoms of the data subject."

This assessment may take on greater weight, experts said, as action by other organizations gathers steam. The CNIL decision came after two associations – privacy activist Max Schrems' Vienna-based NOYB (short for, "None of Your Business") and the French nonprofit La Quadrature du Net – lodged complaints about Google's processing of personal information. Other consumer advocacy groups are expected to follow suit.

"Although global technology companies are likely the initial and primary targets of their complaints, all industries are exposed to their [consumer groups'] newfound powers under GDPR," said Rita S. Heimes, general counsel and research director of the International Association of Privacy Professionals.

Beyond cementing consumer advocacy groups' right to advocate for data subjects, the CNIL decision places limits on GDPR's one-stop-shop mechanism. The intent of OSS was to allow organizations engaged in cross-border data processing to have claims reviewed by a single data protection authority based on the location of the data controller's "main establishment" in the EU.

Google argued that its main establishment was in Ireland, suggesting the case be brought before the Irish Data Protection Commission, but CNIL stated the office had no decision-making authority over Google's data processing operations. This strict interpretation of a "lead supervisory authority" by CNIL also merits corporate consideration.

All industries are exposed to consumer groups' newfound power under GDPR.

"This may mean that just appointing a representative – or even having an office in the EU – will not necessarily trigger one-stop shop," Heimes said.

In the meantime, businesses need to proceed with caution, ITIF's Castro said. "Companies should know that European regulators are paying close attention to complaints and not letting off first-time violators with just a warning. Any violation can result in a serious fine."

Nor will the scythe cut only the tallest grass. Beyond Google, CNIL leveled a fine against a French startup in October. Companies large and small are on notice.

"The CNIL decision is a wake-up call to review existing privacy policies, cookie notices, and banners to ensure that consents are specific and informed," McKean said.

For general counsel, "the most important step is to understand not only all of their organization's data processing activities, but the lawful basis for each one," Heimes said.

"If consent is the only appropriate basis for an activity, counsel should make sure [it] is acquired through a clear and affirmative opt-in statement, with no pre-ticked boxes, accompanied by a simple statement of what the consent is for, with mechanisms in place to track the consent and allow for its withdrawal," Heimes said. "Vague and generic statements will not suffice."

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

Tougher Laws Will Bring More Class-Action Litigation

By Shaheen Pasha

Recent high-profile lawsuits and tougher privacy legislation coming out of California are expected to create a new wave of class-action litigation in specialized technology industries and other areas heavily reliant on personal data.

The California Consumer Privacy Act is slated to become one of the toughest privacy laws in the country, requiring significantly more transparency in how companies collect, use, and disclose personal information.

The law will go into effect on Jan. 1, 2020, and will impact roughly 500,000 businesses that collect and sell personal information or disclose it for business purposes, according to the International Association of Privacy Professionals. That includes small and mid-size businesses, as well as the major tech players in Silicon Valley.

The California statute establishes a private right of action for breaches, according to Bloomberg Law.

The new law was hailed as a win for individual consumers to better protect their privacy in the wake of data breaches at companies such as Target, Equifax, and Cambridge Analytica that affected millions of Americans. But it will be costly and complicated to implement for businesses. A recent survey conducted by privacy compliance firm TrustArc found 86 percent of companies surveyed had not completed the compliance process, and 44 percent had not even begun implementation.

That raises concerns over business readiness and opens the door for lawsuits against corporations once the legislation takes effect.

"For the past several years, the plaintiffs' bar has been in search of something in litigation that would have a payout, which has been elusive in data privacy cases," said Matthew Prewitt, lead of the data privacy and cyber security practice at Schiff Hardin. "Unless there is a federal statute of general application that preempts the California statute, it seems highly likely that this time next year, there will be a much more robust plaintiffs' bar ready to commence plaintiff action."

As currently written, the new law establishes a private right of action for security breaches and sets damages of $100 to $750 per consumer, per incident. In addition, the attorney general can file cases against the company for up to $7,500 per violation. But there are amendments in the works that could pave the way for more lawsuits.

Proposed amendments filed in February would broaden consumers' "right to private action" and remove language that would allow business a free pass to "cure" violations before an enforcement could occur. The attorney general would also not be required to provide companies and private parties with legal counsel on CCPA compliance at taxpayer expense.

This is just the beginning. Many see the CCPA as a model for other states. According to Bloomberg Law, Massachusetts, Rhode Island, New York, and Washington are all floating similar proposals. Prewitt said that, in the absence of a federal statute and given that California constitutes such a large portion of the U.S. economy, California's data privacy law could well become the default for the rest of the states.

And lawsuits will follow. In other areas of privacy law, litigation is already on the rise. A January court ruling in Illinois found consumers don't have to show specific harm in order to sue companies under the state's Biometric Information Privacy Act. Since then, there has been an explosion in biometric privacy litigation over the use of personal data, resulting in law firms forming new practice groups and hiring lawyers to meet the demand, according to Bloomberg Law.

"BIPA is similar as a statute to California's law as it provides civil remedy that doesn't require separate showing of harm," Prewitt said. "The CCPA, as it is written, seems to provide a strong catalyst for data breach litigation. There's money to be had if you can prove a breach, and that's classic fodder for litigation."

It's a landscape that some legal experts worry will stifle innovation and curb business in the U.S. Mark Mao, co-lead of the privacy practice at Troutman Sanders, said that measures such as the CCPA and its European counterpart, the General Data Protection Regulation, are introducing vague laws that increase liability and compliance issues that will deter companies from developing technology, which is critical for international competition.

A federal solution needs to emerge to simplify the process for business.

"Here in the U.S., the landscape around connective technology like electric vehicles, connected devices, and other emerging technologies is becoming increasingly controversial," Mao said.

"That's making it harder for us to stay competitive in business internationally. In Europe, the GDPR was passed, and the legislators are feeling good about themselves for passing such a comprehensive law. But it's getting harder to get tech companies into countries like France and Germany. They're seeing a giant brain suck."

Mao said such a scenario is likely in the U.S. if individual states pass similar data privacy laws. He added that a federal solution will need to emerge to simplify the process for corporations.

That's what the Federal Trade Commission is advocating. "The best thing we can do for privacy" is pass a national data breach law, FTC Commissioner Noah Phillips said at the Brookings Institution in March, according to Bloomberg Law.

He said multiple laws across 51 states and territories muddy privacy compliance and called for rulemaking authority to lie with Congress, focusing more on privacy issues surrounding the Health Insurance Portability and Accountability Act and the Children's Online Privacy Protection Act, rather than creating broad, anticompetitive privacy legislation.

The House Energy and Commerce Committee met in February to discuss federal regulation on data privacy, with states expressing concern that a federal law would preempt and weaken state regulation, while tech companies worried that giving too much power to the states to regulate privacy would hinder business.

Shaheen Pasha is a writer and journalism professor, focusing on legal and financial issues.

Companies Anxious for Federal Move on Privacy

By Andrew Bowyer

The implementation of the EU's General Data Protection Regulation in May 2018 and a series of breaches and cases of data misuse by companies raise concerns about the future of privacy regulation in the U.S.

As it now stands, companies must be prepared to deal not only with the requirements imposed by GDPR, but also with a patchwork of state laws that may carry compliance requirements as well. Many experts are calling for a unified federal statute that addresses the collection, use, sharing, and destruction of personal information and the consumer's rights that attach.

California's Consumer Privacy Act presents challenges to many businesses and legal practitioners, according to Bloomberg Law.

Given that any comprehensive federal legislation is unlikely until at least sometime next year, the California Consumer Privacy Act is effectively the model that is being anticipated. The legislation, which takes effect next year, is comprehensive in scope and in many ways reflects the overall approach taken by GDPR.

But CCPA presents many challenges. Businesses and legal practitioners claim it was rushed through the approval process without sufficient input from stakeholders. Other complaints are that it works against the privacy of personal information and imposes an unfair level of compliance expense on small businesses. And inconsistencies between the act and GDPR mean that having prepared for the latter's requirements will be of little help to firms when they face the California provisions.

To open a dialogue to help move toward a federal statute, Intel last November published a privacy bill draft and set up a website to receive comments. Reflecting the interests of tech companies that purchase its chips, Intel's proposal incorporates the premise that a consumer-focused regulatory approach embodying the "notice and choice" found in both GDPR and CCPA will be harmful to continuing innovation.

Leaders in the tech sector also think both measures will undermine consumer privacy because to enable the required access, erasure, and portability of personal information, businesses will need to make all their data identifiable — even what they might otherwise be able to store in non-identifiable ways.

"The burden should be on companies over the consumer in managing data," said David Hoffman, associate general counsel and global privacy officer at Intel. "What's going to be critical is that their model [federal laws] is a stronger and better bill of CCPA.

"Conversation is trending toward CCPA as a floor. What we really need is … stronger protection for privacy. CCPA as a notice-and-choice approach really doesn't do that."

Hoffman added that consumers don't have time to read policies and aren't aware of exactly how their data will be collected and used, and that it makes more sense for companies to be responsible for this.

Uncertainty over the course of privacy regulation will be a given until a comprehensive federal statute is enacted.

"We're in the midst of a large public policy debate about what we're going to do when it comes to data privacy laws," said Colin Zick, a privacy partner at Foley Hoag in Boston. "It's rare when we see this kind of situation where it's not at all clear where things are going.

"Industry is basically saying, please regulate us because we really don't want California to regulate us," Zick said, referring to aspects of CCPA that companies fear may be costly, difficult to comply with, and not provide adequately for data privacy.

The Intel proposal addresses a key criticism of CCPA: that it's broadly applied across all industries, with few exceptions, counter to the belief that privacy issues need to be considered on a sector-by-sector basis. The Intel offering defines a carve-out for companies with fewer than 25 employees, those that collect or use the personal data of fewer than 50,000 individuals, or those that derive less than half of all revenue annually from the sale of personal data. This would effectively eliminate companies whose core business is not data-focused from being regulated by privacy laws.

Privacy regulation will be uncertain until a federal statute is passed.

The other side of the proposal is a regulatory requirement based on company type and size. The same scale across the board could be destructive to small firms because of the relative burden of compliance costs.

"If you're a large-scale organization, you should be accountable," Hoffman said. "What will get in the way of small businesses' competitiveness is having a patchwork of legislation where they will have to engage large law firms in order to comply. This will have a real impact on their competitiveness."

The Intel approach also would implement the Fair Information and Privacy Principles laid out by the Organization for Economic Cooperation and Development, which Hoffman said are better guidance than that offered by the European or California regulations. He notes in particular the OECD's use-limitation and accountability features incorporated in the Intel draft.

In the absence of a federal statute emerging, legal action at the state level may drive the process.

"From the attorney general perspective, it will be through the lens of consumers having choice," said Bill McCollum, who served as Florida's attorney general and is now co-chair of Dentons' state attorney general practice.

State attorneys general will have to make a balancing call, offering consumers the opportunity to choose how their data is collected and shared by companies, he said. On the other hand, if the consumer is given too many choices, it will be difficult to balance, and if it's overdone it could be harmful to the business models of these companies.

McCollum noted state attorneys general also may focus on the type of business the regulated companies are in and the value they add. "There may be some room for deviation," he said, "depending on the nature of the business model and the public good it provides."

Andrew Bowyer writes and convenes forums on the business of law and legal technology.

Bloomberg Law®