‘The Internet Is Fractured’: Experts Talk Compliance Regulation Challenges

Ray Fernandez
February 26, 2024

The number of laws that affect digital operations worldwide is overwhelming — and sometimes contradictory.
From European laws, such as the General Data Protection Regulation (GDPR), to federal and state laws in the US, such as the California Consumer Privacy Act (CCPA), keeping up with compliance while avoiding cybersecurity breaches, fines, and legal actions is becoming every day more challenging for business owners and IT leaders.

The constant evolution and jurisdictional variance of the legal landscape, along with new technologies like generative AI — giving birth to more regulations such as the incoming EU AI Act — muddies the compliance complexity waters further.

Techopedia talked to experts in the field to understand the state of global compliance, how it challenges companies, and what actionable solutions businesses and leaders can take today.

Key Takeaways

- It’s a global internet — but every business is bound by the laws where they operate and where their customers and employees are.
- However, the compliance landscape is chaotic — with legislation from international, national, and even at a state level sometimes contradicting each other.
- The burden falls heavily on companies to decipher the tangled web of laws and standards across borders, with penalties for those who fail to keep up.
- Techopedia canvasses a wide range of expert opinions – is there a solution, even as new laws, including AI regulations, come online every day? And can cloud service providers do more to help?

Understanding Challenges and Opportunities

The recent VinciWorks January 2024 survey reveals that 44% of compliance professionals admit to being unprepared for 2024 challenges. According to the study, only 7% feel fully confident in tackling the challenges of an ever-changing regulatory landscape.

In a note to Techopedia, Ruoting Sun, VP of Product, Secureframe — an automated and AI-powered compliance company built by compliance experts — explained that laws often overlap, giving way to different interpretations and regional variations:

“Interpretations and expectations of user privacy and security vary significantly among different countries and regions. The centralized and connected model of the internet doesn’t align well with the fragmented needs of various nation-states or even individual American states.”

Lisa McStay, Chief Operating Officer at Continuity2, encounters global and regional compliance challenges on a daily basis.

She told Techopedia:

“The internet is fractured when it comes to digital laws. (For example), the USA’s CCPA and Canada’s PIPEDA have implemented some of the EU’s GDPR rules. The three have distinct differences in their implementation, which creates an unbalanced governance around the digital world.”

McStay explains that countries monitor the internet and data use and then decide on what regulations to insert, creating a naturally uneven landscape.

“Adding to this, in the US, sectors have patchwork laws instead of one overarching law like many other countries. This makes it even more difficult, especially for international businesses.”

It´s Not Just Laws but Standards, Too

Arik Solomon, CEO and Co-founder of Cypago — enabling companies to streamline and automate their processes and workflows around cyber governance, risk, and compliance (GRC) — told Techopedia that it is not just laws that affect companies and IT operations.

“Apart from data privacy laws like GDPR, CCPA, and PIPEDA, various compliance frameworks exist, such as SOC 2, ISO 27001, HIPAA, and others. Each with its own set of requirements and standards. These frameworks often overlap but can also have unique aspects that add to the complexity for companies operating in multiple jurisdictions.”

Solomon explained that under this scenario, a company may need to comply with GDPR in Europe while also adhering to SOC 2 standards for its services. Additionally, the CLOUD Act, for example, also directly contradicts the GDPR in some aspects, presenting real issues for anyone operating with US-based servers.

“Managing and aligning these diverse compliance requirements can be challenging and contribute to the fragmentation of regulatory landscapes on the internet.”

A Shift In Perception: From Crisis to Opportunities

Jodi Daniels, founder and CEO of Red Clover Advisors, Faculty member at IANS Research, and privacy advisor expert in GDPR, CCPA, and US privacy laws, sees opportunities in this compliance crisis.

“Companies collect, use, and share data because they can and the focus has been on the company first, individual second. Now that is changing, companies have to consider the individual first.”

Daniels said that privacy laws are designed to protect individuals and not to harm companies. Daniels explained that while companies face the challenges of adapting at first — which in the short term affects their performance — in the long run, businesses will work alongside privacy laws just like they do with financial, tax, HR, and other laws.

The Hidden Costs of Compliance

The global impact of compliance makes it almost impossible to quantify the total costs that businesses and organizations face around the world every year.

A recent report from the CATO Institute concluded that in the US, a firm spends between

1.3 and 3.3 % of its total wage bill on regulatory compliance — with this percentage being higher for firms with around 500 employees.

LexisNexis Risk Solutions adds that the global cost of financial crime compliance alone — affecting nearly every financial institution — has skyrocketed in the past year, reaching a total cost of $206.1 billion.

But from burnout to business reputation damages, compliance costs go well beyond numbers on the bottom line, affecting business owners, executives, IT staff, and end users. Leading companies are building up GRC teams, investing in new technology, and leveraging automation and AI to bring down compliance costs.

Building Up GRC Teams

McStay explained why building up GRC teams is a number one priority.

“The dominant impact GRC teams face is the increase in resources needed to cover the variety of rules and laws from around the world.”

McStay added that GRC teams need to be highly skilled, specifically when working in international businesses. They must also be familiar with new digital laws that are continually emerging at all levels.

Sun from Secureframe recognized that compliance could complicate business expansion significantly but urged businesses to devise a coherent, unified framework that can help them interpret and adhere to the diverse array of laws dictated by the countries in which companies operate. GRC teams are ultimately the people who will develop and execute this framework.

Solomon also spoke about the need for businesses to invest substantially, adding that compliance challenges not only slow down operations but also escalate costs and potentially constrain market expansion.

"To address these challenges, GRC teams should stay informed about evolving regulations, establish clear governance structures, invest in technology solutions, foster collaboration across departments, and engage with regulatory authorities.

"This proactive approach enables GRC teams to navigate the complexities of fractured digital laws effectively, enhance compliance efforts, and mitigate associated risks."

Google, Amazon, Microsoft, and other Cloud Providers Could do More

Cloud providers have invested heavily in compliance, integrating into their cloud portfolios innovative tools and technologies such as AI-driven compliance and machine learning automation.

However you choose your cloud provider, Sun believes that in our post-digital transformation era, where almost every sector and type of business operates in the cloud, companies like Google Cloud Platform, Microsoft Azure, Amazon Web Services, IBM, and Oracle Cloud could do more.

"Cloud providers alleviate much of the infrastructure-building burden for individual companies seeking expansion into new markets.

"The more they [cloud providers] can do to address regional differences in privacy and security interpretations, the less compliance responsibility falls on the customers operating within those public clouds."

Sun explained that new cloud digital infrastructures could also be a solution. For example, engineering public cloud infrastructure for specific regions, such as for US federal versus commercial customers, EU customers, ANZ customers, and others.

"These clouds (could) not only operate differently, depending on the region, but also have varying data privacy, security, and retention policies to comply with regional regulations."

Solomon agreed with Sun and added that as leaders in cloud computing services, top cloud providers have the resources and expertise to help businesses navigate complex regulatory landscapes across different regions.

Solomon also voiced in favor of pre-built, compliance-ready configurations integrated into public cloud platforms.

"This (would) include features such as data encryption, access controls, and audit logging that align with various regulatory requirements. They can also invest in aligning their global footprint and data centers with regional data privacy laws and other regulatory frameworks."

The Era of AI and Automation in Compliance

New compliance automated technologies integrated into Customer Relationship Management (CRM) management tools, human resources information systems (HRIS), and other business platforms are becoming the norm.

Additionally, as in any other sector, AI is viewed by compliance officers as a resource that has significant potential to streamline governance. While AI is relatively new in the field, companies are already adopting the technology, Sun said.

"We observe a growing trend of traditional infosec compliance operations becoming automated," Sun said. "Much of today's infosec tooling, where compliance evidence resides, is cloud-hosted and offers robust APIs for data exchange, enabling automation and continuous monitoring."

"Additionally, AI shows tremendous promise in helping organizations identify gaps in their compliance programs, rectify security misconfigurations, streamline vendor assessments and procurement processes, and more."

Keeping Humans In The Loop

Despite the potential and inevitable widespread of AI compliance, innovation does not come without risks. Human talent and issues like AI bias or machine model drift, as well as oversight and verification of any AI´s performance, are essential factors.

Daniels from IANS explained how and in what cases businesses can deploy AI and stressed the importance of including human in the loop.

"AI can be helpful in identifying data in discovery tools or flagging potential privacy risks. It should be used in conjunction with human review and not 100% relied upon.

"Nuance and specific use cases are not always flagged by tools and interpretation plus strategic decision-making should happen at the human level, not just a computer."

Solomon — a firm believer in the power of AI and automation — said: "By harnessing the capabilities of automation and AI, we can empower GRC teams to focus on higher-value tasks such as risk analysis and mitigation.

"Automation enables real-time monitoring and enforcement of compliance policies, ensuring continuous adherence to regulatory requirements.

"This proactive approach strengthens an organization's compliance posture and reduces the likelihood of costly violations or breaches."

The Future of Compliance

The ever-changing nature of global compliance makes it almost impossible for business owners and tech workers to imagine the future for the sector in five or ten years. However, envisioning the future of this complex global landscape is not only vital but can help companies better prepare and design strategic development plans.

McStay believes that technology is the key to the future of compliance.

“Businesses will adopt and use more sophisticated technology, possibly tools which use AI and machine learning to streamline the compliance process across the business. Such tools would also be great for updating businesses when laws and regulations change.”

On the other hand, Daniels spoke about embedded and integrated technologies and a future where privacy laws include everyone around the world.

“Security and compliance will be embedded into all data use cases from engineering at the beginning to notice disclosures, and systems will be integrated so honoring individual rights requests will not be so manual or ad-hoc as they are today.

“Privacy laws will no longer be an afterthought, and most people globally will be covered by privacy laws.”

In contrast, Solomon, despite recognizing that AI and automation will make processes smoother and more effective, said compliance and security will undergo a profound transformation.

“Emerging digital laws will necessitate a paradigm shift towards a more integrated and interconnected approach. Businesses will have to get creative and blend compliance rules with their security measures.”

The Bottom Line

The compliance challenges of the future and of today are, without doubt, monumental. However, focusing on solutions and generating change to drive efficiency is possible.

Investing in new tech, building up GRC teams, up-skilling workers, and deploying AI systems that include humans in the loop, can help businesses of all sizes overcome the roadblocks of meeting regulations and strengthening their security posture.

IT leaders can also benefit by leveraging the existing cybersecurity and compliance resources that cloud providers offer embedded into their products.

Additionally, experts agree that new public cloud structures — designed with regional compliance at their core — could benefit companies and organizations. Those who will emerge at the top of compliance and security management are those who seek and find opportunities and take action on solutions despite the complexities.