REPRINT

R&C risk & compliance

PRIVACY AND ENTERPRISE RISK MANAGEMENT

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2019 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

PROMONTORY
an IBM Company

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

www.riskandcompliancemagazine.com

PERSPECTIVES

PRIVACY AND ENTERPRISE RISK MANAGEMENT

BY **EUGENE LUDWIG AND LEIGH FELDMAN**
> PROMONTORY FINANCIAL GROUP

The key takeaway from recent privacy-related missteps is that organisations should be laser-focused on how they use personal data. In the last couple of years, we have seen privacy issues impact company valuations and brand trust. Organisations have stumbled due to a lack of transparency, excessive personal data collection, ignoring consumer privacy choices and retaining information longer than necessary. In addition, algorithms have recently emerged that assume biased and racist characteristics. Not surprisingly, the news coverage on privacy has moved from the technology section, to the business section, to the front page.

Governments have already responded with comprehensive privacy regulations, including the General Data Protection Regulation (GDPR) in Europe and the recently-passed California Consumer Privacy Act (CCPA) in the US. These laws are beginning to put a more comprehensive framework around data collection, processing and sharing, and are creating many new obligations and responsibilities for organisations. Penalties for privacy violations are also increasing, with the GDPR imposing penalties on violators of the greater of up to 4 percent of global revenue or €20m. Countries around the world are now considering similar updates to their own versions of data privacy regulation.

On top of all of this, organisations are rapidly deploying advanced technologies, including Big Data analytics, artificial intelligence (AI), blockchain and cloud storage and computing, to name just a few, where the responsible use of information is essential. This environment begs the questions: What should organisations do to avoid mistakes? And what should they do to gain a competitive advantage?

While organisations are working to comply with these new, more complex, and sometimes inconsistent global privacy laws, discussions around privacy are quickly moving beyond historical understandings of privacy harms and into broader questions of responsible information processing. In light of these growing concerns over the responsible use of data, digital ethics is emerging as a discrete topic. As organisations use increasingly sophisticated technologies to capture and process data, they must focus on not only implementing appropriate transparency and user-choice controls, but also addressing concepts such as bias in data sets, discriminatory effects and societal impacts.

Financial institutions have looked at some of these issues in disparate ways across privacy, fair lending, unfair, deceptive or abusive acts or practices (UDAAP), data governance, model development and conduct programmes. It is now important, however, to bring these strands together and view them through a single digital ethics lens to support compliance and business development in the emerging distributed, digital banking landscape.

"All organisations should be prioritising privacy considerations for customers and other stakeholders through a broader, yet more nuanced lens."

Other, less-regulated industries will also need to get up to speed quickly as they deploy more advanced technologies and data-processing capabilities. Otherwise, they risk runaway algorithms making determinations that are ethically questionable and contrary to company standards, customer expectations and societal norms.

As we move further into a more connected and smart technology landscape, organisations will need to consider consumer and governmental concerns about whether the use of data is legally-compliant, responsible and ethical. Organisations must be cognisant that their legal ability to do something with data does not mean it is ethically or socially permissible. Individuals are becoming increasingly

concerned about their personal information. All organisations should be prioritising privacy considerations for customers and other stakeholders through a broader, yet more nuanced lens.

In response to these rapid changes in the privacy landscape, regulatory compliance remains critical, and will likely need to be enhanced to address new global privacy laws and regulations. However, beyond just compliance, organisations should begin to see their privacy programmes as business imperatives. Comprehensive privacy programmes, with a digital ethics focus, will be critical in meeting customer expectations, supporting brand values and enabling rapid innovation.

Additionally, organisations across multiple industries should establish new mechanisms within or adjacent to their privacy programmes. This includes augmenting privacy impact assessments

with additional, focused digital ethics reviews, including policies, assessments, bias detection tools and output testing, to address issues that go beyond traditional privacy compliance matters. This will also be necessary for organisations to maximise and optimise how they collect and use data to drive their businesses. The ability to quickly answer questions about responsible data collection, access, use and sharing, as well as how to optimise global data movement, will speed up product research and development and overall business activity. An organisation that can clear privacy-related questions in days will have an advantage compared to organisations where those decisions can take weeks or months.

As society moves into the AI age, failure to collect and process information responsibly, transparently and in compliance with increasingly complex global privacy regulations and expectations could threaten business survival. On the flip side, the appropriate and effective management and utilisation of data will increase customer trust and could enhance market power and revenue.

All of this portends a seismic shift in how organisations approach privacy and enterprise risk management. Organisations that do not make this transition will be more likely to face regulatory issues and public relations failures. They will also be less efficient with data and slower to market with new information-based products and services. Organisations that are able to upgrade their privacy programmes to provide rapid, flexible and risk-based regulatory compliance, coupled with the ability to assess whether data use is ethical, will be better positioned to steer clear of regulatory pitfalls and reap AI-age rewards. R&C

Eugene Ludwig
Founder and Chief Executive Officer
Promontory Financial Group
T: +1 (202) 384 1200
E: eludwig@promontory.com

Eugene Ludwig, the founder and chief executive officer of Promontory Financial Group, is a trusted adviser to many of the world's leading financial companies. He is widely recognised as a farsighted thinker on the most pressing issues confronting financial services. Before founding Promontory, he served under president Clinton as US comptroller of the currency, the head of the federal agency responsible for supervising the preponderance of US banking assets. He went on to become vice chairman and senior control officer of Bankers Trust/ Deutsche Bank.

Leigh Feldman
Managing Director
Promontory Financial Group
T: +1 (212) 365 6976
E: lfeldman@promontory.com

Leigh Feldman is an expert in privacy and data protection who leads Promontory's US privacy practice, advising clients on all aspects of privacy programmes, frameworks and topics, including issues related to Big Data, cloud computing, blockchain, digital ethics and artificial intelligence. Prior to joining Promontory, he led Citigroup's privacy function and served as co-chair of the bank's General Data Protection Regulation steering committee. Previously, Mr Feldman was also chief privacy officer at American Express, and before that, he led Bank of America's privacy team.