REPRINT

R&C risk & compliance

# DATA ANALYTICS AND DATA PRIVACY

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2019 ISSUE


www.riskandcompliancemagazine.com

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

NAVIGANT

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

MINI-ROUNDTABLE

# DATA ANALYTICS AND DATA PRIVACY

## PANEL EXPERTS

**Joseph Campbell**
Director, Global Investigations & Compliance
Navigant Consulting
T: +1 (202) 973 4595
E: joseph.campbell@navigant.com

**Joseph Campbell** is a director in Navigant's global investigations & compliance practice, where his role involves leading anti-bribery and corruption, anti-money laundering and financial investigations. He has significant experience in the investigation and assessment of cross-border tax matters through review and analysis of business and financial institution international investments and transactions regarding global corporations and financial institutions. Additionally, he has led reviews of the business processes and internal controls of global companies regarding financial and accounting practices and anti-corruption measures.

**Kathryn Rock**
Director, Banking Insurance and Capital Markets
Navigant Consulting, Inc.
T: +1 (202) 973 6541
E: krock@navigant.com

**Kathryn Rock** is a director within the banking, insurance & capital markets practice at Navigant. Ms Rock has over 16 years of experience advising banking and government organisations and auditing various financial services clients. She has been a speaker at events and on webinars related to the California Consumer Privacy Act (CCPA) and has conducted training on the CCPA for a large financial institution. Prior to her time at Navigant, Ms Rock was an accomplished audit professional at a Big Four professional services firm. She performed external audits for multiple financial services clients.

**Catherine Meyer**
Senior Counsel
Pillsbury Winthrop Shaw Pittman LLP
T: +1 (213) 488 7362
E: catherine.meyer@pillsburylaw.com

**Catherine Meyer** is recognised by *Legal 500 US* as an authority on data protection, privacy and cyber law. She advises clients on compliance with state, federal and international data protection and privacy statutes and regulations regarding the collection, use, sale, transfer and sharing of customer information for commercial purposes, including the GDPR and the California Consumer Privacy Act, she assists when personal information is compromised and advises on responding to data breaches.

**R&C: Could you provide an overview of data privacy trends unfolding across the globe? What have been the overarching developments of the past few years?**

**Campbell:** Countries and their citizens recognise the critical importance of information privacy. Compromised personal data is exploited by malicious actors to victimise individuals through financial and identity fraud and used against countries' economic and national security interests. Data compromises include breaches such as the 2015 identified cyber penetration of the US Office of Personnel Management. Other noteworthy data breaches include Marriott Starwood Hotels, Quora, Google and T-Mobile. Beyond the European Union's (EU's) General Data Protection Regulation (GDPR), approximately 80 countries have instituted data privacy laws, including the US, through laws such as the Health Insurance Portability and Accountability Act and the Driver's Privacy Protection Act of 1994. Only California has passed a specific consumer privacy law, the 2018 California Consumer Privacy Act (CCPA). Many other states are considering the passage of similar laws. Colorado and Iowa have already strengthened their protection of consumer and student information, respectively.

**Meyer:** The EU's adoption of the GDPR exemplifies the trend in data privacy toward more transparency in how businesses use and monetise data and more individual control over the use and exploitation of personal information. The GDPR follows the May 2017 amendment to Japan's Act on the Protection of Personal Information, which expanded its application to include foreign as well as domestic companies and the Privacy Amendment (Notifiable Data Breaches) to Australia's Privacy Act, effective in February 2018, which strengthened consequences for exposure of personal information resulting from lax security. Brazil's General Law of Data Protection, effective February 2020, substantially mirrors the GDPR in scope and fines, and is another example of this growing trend. The CCPA, effective 1 January 2020, is an example of a US state legislature's effort to increase transparency and individual control over data use.

**Rock:** Revelations about the ways consumer data is collected, stored and used from highly publicised events, such as the Cambridge Analytica scandal in the US, have placed a spotlight on companies' data privacy policies and governing regulations. Countries all over the world have been enacting data privacy laws or more comprehensive ones where such laws already exist. The EU's GDPR has received a lot of recognition; however, Brazil, Canada and Japan, among others, have also passed key laws. In the US, the CCPA has passed, while states such as Washington and Texas are advancing their own legislation. This has sparked discussion over which

US regulatory body is best suited for oversight, with the Federal Trade Commission (FTC) currently providing consumer protection oversight. Regulators across the globe are beginning to take action, as indicated by France's nearly $57m fine of Google for violating GDPR.

**R&C: How would you describe the impact of two key pieces of legislation – the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)? To what extent are these privacy laws shaking up how companies collect and process data?**

**Meyer:** The GDPR and the CCPA are forcing businesses to examine their collection and use of personal data. The requirements under each for extensive disclosure of how data is used by a company provide increased transparency that allows individuals to choose how they interact with the company. The rights of individuals to receive a copy of the specific pieces of information collected by a company, to have their information deleted, and to limit how their information is processed or sold, are a dramatic shift away from a company's former ability to amass large quantities of personal data. It remains to be seen whether the obligations imposed on businesses by the GDPR and the CCPA will result in any changes in their commercial behaviour with respect to data collection and use.

**Rock:** As a result of both the GDPR and the CCPA, companies must be more transparent and assume more responsibility regarding the collection and processing of any consumer personal information. Companies need to understand the consumer data they collect and have in their possession, along with the various ways it is used, including any interactions with third parties. Companies are being held accountable for how they interact with personal information and that has translated into adjustments to their business processes related to data collection and use, particularly as both pieces of legislation allow for financial penalties to be levied on any companies found to be in violation. Particularly, the CCPA's private right of action explicitly allows

> **"The CCPA, effective 1 January 2020, is an example of a US state legislature's effort to increase transparency and individual control over data use."**
>
> *Catherine Meyer, Pillsbury Winthrop Shaw Pittman LLP*

consumers to seek damages for any violations of the CCPA, which exposes companies to both civil penalties levied by regulators and damages paid directly to consumers.

**R&C: Drilling down, what are the key features and provisions of the GDPR and the CCPA?**

**Rock:** Among other things, the GDPR and the CCPA provide consumers with certain rights related to their personal information, namely the rights to access and obtain copies of their information, to request erasure of their information – known as the right to be forgotten – and to seek legal recourse. Additionally, both provide for civil penalties that can be assessed to companies found to be in violation of either law. There are some notable differences, however. The GDPR pertains to information processed by a company, while the CCPA pertains to information collected. Additionally, the CCPA expands the definition of personal data to that which can be associated to a household, not just an individual. The GDPR requires more organisational standards, such as requiring a data protection officer (DPO) in some situations, considering data privacy when undertaking new initiatives, such as data protection by design, and performing risk assessments of data processing systems. The CCPA does not explicitly require any of these actions.

**Meyer:** Expanded disclosures, including sources, uses and sharing practices relating to broad categories of personal information, data portability, data erasure and restrictions on processing or sale of data are the key features of the GDPR and CCPA. While the two regulations differ in scope and application in some significant ways, the policy behind both is consistent: increased transparency and increased individual control. The right of rectification, which is unique to the GDPR, and the right of non-discrimination, which is unique to the CCPA, serve to protect the accuracy of data held by a company and to prohibit retaliation for the exercise of new individual rights.

> **"Many companies have been gathering data for analytical purposes for many years as the concept of Big Data has become more prevalent."**
>
> *Kathryn Rock, Navigant Consulting, Inc.*

**R&C: How would you characterise the growing intersection between data analytics and data privacy? In your experience, do companies tend to underestimate the data privacy implications of conducting data analytics?**

**Meyer:** More tools are being made available to businesses that facilitate the organisation and interpretation of data in order to present the data in context, as well as in a format that is useful to the business. Data analytics gives the business the ability to analyse data about products, services and the operation of the business. Information about consumer behaviour is highly valued so that product marketing can be more efficient and effective. The demand for such behavioural data often overshadows consumers' data privacy expectations, however. Globally, new regulations are demanding that businesses take into consideration those privacy expectations when employing data analytics technology.

**Rock:** Many companies have been gathering data for analytical purposes for many years as the concept of Big Data has become more prevalent. Data analytics allow companies to identify patterns and predict behaviour, which helps them design and market more targeted products to consumers, among other items. However, most of these companies, even the largest ones, have not fully considered the implications of data privacy in holding all this information. In fact, holding on to unnecessary or unused data poses additional risks to these companies as these new data privacy laws go into effect and regulators begin to hold businesses accountable for any violations or data breaches. Companies may want to consider assessing the amount of data they really need and utilise, and then eliminate unnecessary or unused data.

**Campbell:** Businesses increasingly require consumer data to effectively design and market products and address customer needs. Businesses collect data of purchases, extending into the realm of the Internet of Things (IoT), and monitor real-time product use and performance. All data is analysed to improve service and maximise profit. Businesses must be attuned to GDPR and CCPA requirements regarding the management of customer data ingested from a variety of sources. A data inventory should be maintained to ensure compliance with customer rights. Companies should have a solid information security programme that protects data confidentiality in order to prevent disclosure to unauthorised parties, integrity which will protect information from being modified, and availability which will ensure that authorised parties can access information when needed. Over half of all states have enacted data disposal laws. Companies should also have data disposal programmes, in line with laws

and regulations, to dispose of data no longer needed, further protecting consumers from data breach consequences.

**R&C: With companies turning to data analytics with increasing frequency, what steps do they need to take to manage related privacy considerations when implementing this technology?**

**Campbell:** Data is power and drives today's businesses. Companies are investing in technologies to collect and process consumer information to benefit product development. Companies should build governance around data privacy, including the development of an information or cyber security programme capable of ensuring that data is properly inventoried, stored, encrypted and monitored to detect internal or external hacking threats. They should demonstrate a commitment to a culture of compliance, driven by top executives through messaging and example. Companies should develop a data privacy team responsible for answering privacy requests and create an audit function to ensure that the company maintains compliance with data privacy laws. Employees should be trained on the laws and their responsibilities in executing procedures to comply with the laws. Companies must also focus on their ability to respond to data leaks, penetration and hacking, in compliance with local laws using a response framework, such as the National Institute of Standards and Technology (NIST) framework, which includes preparation, detection and analysis, containment, eradication and recovery.

**Rock:** Any new technology should be nimble, considering the numerous data privacy laws being enacted or proposed worldwide. Beside assessing if all collected and stored data is necessary, companies can take many steps to manage privacy considerations and risks while implementing technology and utilising data analytics. There are a number of issues companies should consider, the first of which is governance. They should create and update data privacy governance structures and committees to develop and implement strategies for compliance with laws, including the potential inclusion of a chief privacy officer. Companies should also consider policies and procedures. This will require them to develop and update policies and procedures to ensure compliance with existing regulations and implement a robust change management process to account for any new or changing regulations. Training must also be a consideration. Companies must establish and update training programmes to include applicable policies and procedures, including identifying impacted individuals for training. Finally, companies must consider data security. They should review existing data security infrastructure and enhance the organisation's ability to respond to security breaches, in compliance with laws.

**Meyer:** Regulators enforcing data protection laws have focused on privacy by design as a means of addressing data privacy through the development and implementation of technology. This requires embedding privacy protection into the technology and its applications, understanding the scope of data being collected and processed using the technology, and ensuring that the privacy of the data subject is considered at each step in the process. This includes deploying the technology in a way that facilitates the business being able to honour requests from consumers to delete information about them and to limit the processing of their data using the technology.

**R&C: What is your advice to companies on making sure their data usage policies and procedures are as transparent and understandable as possible, so that they do not violate a data subject's right to privacy?**

**Rock:** Companies can do several things to make their data usage policies and procedures as transparent and understandable as possible. Among other items, companies should consider drafting clear policies and procedures, including call scripts, job aides and templates, as well as clear notices and disclosures that can be easily consumed by both internal and external parties, where applicable. These should be updated to account for changing or new regulations on an ongoing, periodic basis. Companies should also prepare and conduct robust data privacy training, including ongoing, periodic training as requirements change or new laws are passed, for all applicable employees. They should also implement and perform ongoing, periodic monitoring of activities, including preparing corrective action plans to address any identified deficiencies and validating the completion of such plans.

> **"Data is power and drives today's businesses."**
>
> *Joseph Campbell, Navigant Consulting*

**Meyer:** Data protection statutes are increasingly requiring the disclosure of all uses of personal data so that individuals are aware of how their information is being used. Data usage policies need to be comprehensive in their disclosures. In addition, they

should be written in clear and easily understood language.

**Campbell:** When building data privacy programmes, companies' data privacy and compliance experts should draft easily accessible policies, with training, to ensure compliance with data privacy laws. Companies can be transparent by publicising their commitment to respecting the data privacy of their customers and employees and how they will do so. Companies can consider issuing a press release and providing details at 'all-hands' meetings regarding their commitment to data privacy and lawful compliance. Companies can also consider sending notices to shareholders, investors and third-party vendors to spell out their data privacy policies and rights. In addition, data privacy should form a part of the company's core values that each employee signs at onboarding and training. Companies should also have practicable systems for data mapping and inventory. This system will be key to ensuring companies respond accurately and quickly to consumer requests related to rights granted within applicable data privacy laws.

**R&C: Going forward, do you believe data privacy concerns will continue to complicate corporate data analytics processes? Are companies likely to struggle to balance these competing interests?**

**Meyer:** There will always be a tension between a business's desire to use personal information for analytics to improve business operations and the protection of the privacy rights of the individuals whose information is impacted. With the trend toward greater transparency and the ability of individuals to demand the deletion of their data, businesses will be looking for alternatives to using identifiable information for analytical purposes. Legislatures, businesses and consumers alike will continue to grapple with this tension.

**Campbell:** Maintaining the privacy and security of data continues to be a challenge for companies that must balance the use of personal information for business processes and profit, with protecting customers and complying with GDPR, CCPA and other privacy-related laws. Without overarching federal legislation, companies must contend with the growing number of state data privacy laws and incorporate related policies and procedures. As JPMorgan Chase chief executive Jamie Dimon noted, "It is imperative that the US government thoughtfully design policies to protect its consumers and that these policies be national versus state-specific". To avoid problems down the road, companies should begin to quickly get educated on applicable privacy laws and develop the underlying governance and strategy. As this is a companywide effort, organisations should be sure to get the right team in place, assign clear roles and responsibilities, conduct

training and begin implementing their data privacy plans without hesitation.

**Rock:** Data privacy is definitely going to continue to add a layer of complexity to data analytics, and companies will undoubtedly struggle to strike the right balance between maintaining large data sets for analytics and protecting consumer data privacy. In the US particularly, this will continue to get more complicated as states issue their own laws in siloes, in lieu of an overarching federal law, which will make compliance challenging for most companies. This is one of the driving forces behind the push for a federal privacy law that is preferred by most organisations. However, until this happens, companies that will be most successful in navigating the evolving global regulatory landscape will be those that have dedicated resources to monitoring evolving laws and requirements, and then translating those into updated policies and procedures, processes and controls. R&C