IADC COMMITTEE NEWSLETTER

CORPORATE COUNSEL

November 2018

IN THIS ISSUE

In this article, the state of EU GDPR compliance relating to developing issues involving blockchain technology and its use in data collection, management, and retention are discussed with a particular view toward in-house counsel's role in compliance and technology innovation evaluation. All counsel who advise companies- large, medium, or small- should read this article as it outlines coming difficulties with disruptive technology on data collection, manipulation, transfer, storage, and security, especially personal data of any type. This is an essential follow up to the recent IADC programs dealing with EU GDPR compliance, blockchain technology's impact on GDPR compliance, and issues involving US data privacy laws and regulations.

What Single Client Counsel Should Know About Worldwide Data Protection and GDPR Compliance

ABOUT THE AUTHOR

Joseph F. Speelman is currently serving as General Counsel for a private, Swiss based energy information group. He has directed successful defense efforts against Public Nuisance lead paint litigation in 15 states, gaining defense verdicts in those states including achieving a defense verdict before the state of Rhode Island Supreme Court that reversed a lower court trial verdict and rendered a defense verdict by the high court. He can be reached at jfspeelman49@gmail.com.

ABOUT THE COMMITTEE

The Corporate Counsel Committee is composed of in-house counsel and others who, although in private practice, serve as general counsel for corporate clients. The Committee provides its members with educational programs and networking opportunities to address common concerns of corporate counsel. It also works to ensure that the IADC and its committees, through their work and offerings, meet the needs of corporate counsel. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article contact:

Alfred R. Paliani
Vice Chair of Publications
Quality King Distributors, Inc.
fpaliani@qkd.com

"Welcome to the tightrope, between the freedom and the chain"
Tightrope
Bob Seger

In the weekend Edition of the Wall Street Journal *[A Global Tech Backlash; Christopher Mims; October 27-28, 2018, Section B, page B4]* some remarkable pieces of information about data protection worldwide were setout from equally remarkable sources. Large tech companies, mostly America's tech giants- Apple, Google, Facebook, and Amazon, to name a few- are experiencing a backlash against their size, power, and how such size and reach affect local, regional, and especially international business operations and conduct. The focus of the article is on data and how these companies handle it….all types of data. *[WSJ, A Global Tech Backlash, cited above.]* While China and its own "tech giants" are included, the brunt of the negative reaction by governments, politicians, employees, and other companies is coming from North America and the EU. *[WSJ, A Global Tech Backlash, cited above]*

The form of negative reaction has been in various proposals to regulate or manage the Internet, including and especially in North America and the EU. EU regulators have rendered a $5 billion fine against Google for exercising monopolistic market conduct. The EU Competition Commissioner is now investigating Amazon as well. At the same time, the Tech companies and major US financial and banking companies are attempting to deal with the impact of the EU General Data Protection Regulation (GDPR) which became effective in May of 2018. Facebook is dealing with a potential EU $1.63 billion fine relating to its admitted personal data breach *[WSJ, A Global Tech Backlash, cited above].*

The GDPR is a sweeping and comprehensive law that has extra-territorial reach similar to the U.S. Foreign Corrupt Practices Act and thus, it has caused significant compliance issues for banking, financial, and credit card groups in the US and Asia. *[WSJ, cited above.]* The US does not have a comprehensive national personal data protection law and some states, such as California, are passing laws similar to the GDPR, causing conflict concerns between national and state law compliance schemes for all companies, small or large, who operate in the US, EU and globally. In essence, there is a perceived compliance related absence in US law on this subject.

In the midst of all this, Apple CEO, Tim Cook, delivered a blistering speech just last week to a data management conference calling for a US data privacy law that parallels and compliments the EU GDPR. Other US companies, such as Google and many commercial banks that rely heavily on data for operations, want something with a "flexible" definition of personal data. Essentially a "watered down" GDPR for the US. Something the EU will not accept. *[WSJ, cited above.]*

A generalized movement of governments, consumer advocates, and political groups around the globe are beginning to focus pressure on large multi-national companies to cede to pressure for strong global data privacy laws as well as limitations on the internet. The potential exists for extended

disputes regarding enforcement of the GDPR and its legal limitations, if any, for extraterritorial administrative and enforcement authority. This is something that in-house counsel should pay very close attention to immediately.

The Role of Single Client Counsel

The backdrop described above creates some very important and complex issues for corporate counsel and their clients. Very difficult and un-clear legal questions and issues are before the in-house counsel in their role as chief legal counselors to all companies operating under the purview of the GDPR, and also in the US with potential data related laws being considered. Issues of corporate governance and decisions regarding dealing with and adequately protecting personal data in the possession of clients arise, irrespective of the presence of applicable regulatory standards on the subject….at least in the litigation prone US legal landscape.

Outside counsel providing legal support on very serious, strategic legal issues of compliance and legal risks related to data management, together with in-house counsel, must determine and deliver advice on these high stakes issues. These are tense and serious times for the single client counsel. In-house counsel, in their risk management and legal counsel roles, must understand these issues and provide correct and timely legal and operational advice to their client. It is unclear how this situation will unfold and legal and compliance risks in the situations described in this article, and the sheer size of such risks are potentially existential to one's client.

To the extent they have not done so, single client counsel must thoroughly understand their client's business operations and business model regarding data management, storage, protection, and use. Further, they must understand the interface their client has in the overall worldwide internet and the security issues they likely have in accumulating, manipulating, and storing external data…most especially personal data. Customer or client financial data, banking data, and related internet information must be adequately protected. Facebook's embarrassing example should have been a "Red Warning Light" on this point to all legal counsel.

Single client counsel have an incredibly important function of risk assessment and management. They have an even more important function to advise their sole client, at the highest level, of the risks that are developing. In this function, counsel should seek out natural allies within the client with which to consult. Chief among those is the accounting function. Accounting professional standards, just as the Attorney Code of Ethics in the legal profession, create professional standards that give guidance and create the duty to communicate directly to the client (in this case corporations) about risks, both potential and actual, through its leadership. It is how the process must work. The process will soon be tested within the international technology giants discussed in this article but also other global companies that are data rich relating to the issue of data protection.

To the single client counsel I offer you the following advice and encouragement… this

process may present professional risks to you. It comes with the territory. Do not shrink from the challenge… embrace it. Yours is not a job….it is an adventure. It is what we do.

The GDPR and Blockchain Technology

The GDPR has become a crystallizing focus process for several issues relating to the internet as well as how data is managed, stored, transmitted, and protected in the internet. As the above and foregoing demonstrates, significant issues exist about the GDPR and its impact. At the same time, much excitement and anticipation has been emerging surrounding the developing technology called "blockchain technology". *[See CLE program materials on Blockchain technology related to the CLE program on the subject during the IADC 2018 Annual Meeting in Lisbon, Portugal in July, 2018].*

While in Lisbon, Portugal, I had dinner with the senior accounting executive for a large, multi-national energy firm headquartered in the EU. When I mentioned the Blockchain technology CLE program, his eye brightened. He indicated that all major, multi-national conglomerates were very excited about the prospect for blockchain to create major improvements in complex, multi-party, multi-jurisdictional commercial contracts that will be a "quantum leap" (his words) for international firms and would allow for significant improvement in contractual formation, processing, and accounting functions. He added a comment to the effect that ensuring blockchain compliance with the EU GDPR needed to be assured. *[personal recollection of J.F. Speelman, July, 2018, Lisbon, Portugal].*

On October 3, 2018, the European Parliament passed a resolution on distributed ledger technologies and blockchain (the "Blockchain Resolution"). The resolution emphasized the importance of taking an "innovation friendly" regulatory approach to ensuring that blockchain technologies comply with the GDPR. *[On the Road to Reconciling GDPR and Blockchain; Michelle Ann Gitlitz & Jennifer Daniels; Blank Rome Publications; Blank Rome LLP; https://www.blankrome.com/publications/road-reconciling-gdpr-and-blockchain, 11/1/18] .*

It appears that significant issues have arisen within the EU GDPR regulatory process regarding blockchain technology compliance with the GDPR. The extraordinary issuance by the European Parliament of a resolution on the issue clearly indicates a rather serious issue with blockchain technology being GDPR compliant. The GDPR mandates that personal data only be processed if there is a lawful basis to do so. It also gives rights to data subjects which provide them significant control over the processing of their personal data. The Parliamentary Resolution, while not carrying the force of law or regulation, does indicate problems with blockchain GDPR compliance. *[Blank Rome publications, Gitlitz & Daniels, On the Road to Reconciling GDPR and Blockchain; cited above.]*

The EU has created an organization, sponsored by the EU Parliament, that is dealing with GDPR compliance especially regarding blockchain database processes. This organization is called the **EU Blockchain Observatory and Forum Initiative of the European Commission.** The group has

published a report on the issues between blockchain technology and GDPR compliance. It provides, in part, the following insight and information:

"Blockchain data base technology enables radical decentralization of data storage and processing and can make it very difficult to interpret some of the GDPR rules and provides technological challenges to GDPR compliance." The paper indicates that **GDPR compliance is not about the technology, it is about how the technology is used.** Just as there is no GDPR compliant internet, or GDPR compliant artificial intelligence algorithm, there is no such thing as a GDPR compliant technology, **there are only GDPR-compliant use cases and applications.** *[Blockchain and the GDPR, A Thematic Report prepared by the European Union Blockchain Observatory and Forum; www.eublockchainforum.eu ; pg 4]*

The report identifies tensions between the GDPR and blockchain technology in three key issues:

- **The identification and obligation of data controllers and processors.** Types of blockchain systems create problems with identifying controllers and compelling them to comply with GDPR privacy mandates.
- **The anonymization of personal data.** There are "intense debates, and currently no consensus" on what is necessary or possible in blockchain to completely remove all personal indicia of individual data information such that it cannot be later recreated. A key requirement to GDPR compliance.
- **The exercise of some data subject rights.** If personal data is recorded in a blockchain network, depending on how it is organized, it may be impossible to rectify or remove such data. The debate centers around a definition of the word "erasure".

In other words, "erase" may not mean "erased", a significant challenge.
[Blockchain and the GDPR; European Union Blockchain Observatory and Forum, cited above.]

To summarize briefly – the essence of the GDPR is to require entities holding, gathering, or storing data from individuals to ensure the data is secure and safe, and if an individual wishes their data removed or erased, such must be done by a designated controller of the data. Blockchain technology cannot, at this point, assure or even allow the above with any certainty as it currently exists and finding a designated controller is difficult or impossible in blockchain technology, depending on who or what organized the blockchain device in the initial stage. These are serious problems. All who have dealt with EU enforcement in bribery, anti-trust or other areas know that the enforcement process is very rigorous. So it is with the GDPR.

All single client counsel whose sole client is doing any level of business in the EU or Switzerland, and which business includes or requires data acquisition, manipulation, transfer, or storage/retention, and such data may contain personal data of individuals, must make themselves and their client aware of the current situation described above and before. If blockchain technology

is involved in the data handling it is essential that counsel advise their client immediately of the issues and information set out above.

If your client is a US entity doing business in the EU or Switzerland, in addition to the above admonition, it is important to ensure the client leadership is aware of Mr. Cook's urging that the US enact a comprehensive data privacy and handling law that mirrors the GDPR. As the Wall Street Journal article cited in this article indicates, the issues are beginning to heat up….everywhere.

As single client counsel, you have only one client….take care of it.

Be Careful Out There.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

MAY 2018
The Single Client Counsel in an Evolving Business Climate
Joseph F. Speelman

MARCH 2018
Corporate Witness Preparation: The 411
Matthew Keenan

What Next Rough Beast….The Second Coming of Nuisance Law Litigation – Part III
Joseph F. Speelman

FEBRUARY 2018
Sponsored Programs at the Midyear Meeting
Joseph F. Speelman

Finding and Closing Judicial Hellholes
Molly Jones and Sherman Joyce

JANUARY 2018
Cyber Security: The Dark Side of the Internet
Joseph F. Speelman

Corporate Counsel Perspectives on Cybersecurity Insurance Procurement
Joseph F. Speelman

OCTOBER 2017
A Tidal Wave of Public Nuisance Law Suits across the US Involving Opioid Litigation
James K. Holder and Joseph F. Speelman

SEPTEMBER2017
What Next Rough Beast….The Second Coming of Nuisance Law Litigation
Joseph F. Speelman

DECEMBER 2016
Please Call Again: The Supreme Court Declines to Rein in TCPA Litigation
W. Jason Rankin and Charles N. Insler

NOVEMBER 2016
No Harm, but Still a Foul? Application of the Supreme Court's Punitive Damages Jurisprudence to Actions Seeking Statutory Damages
Jeffrey A. Holmstrand

OCTOBER 2016
Drone Law and Drone Regulation: A Primer
Lem Montgomery

APRIL 2016
Proportionality and Reasonableness: Using the 2015 FRCP Amendments to Rein in Discovery
Martin J. Healy and Joseph D. Fanning