Published on *The National Law Review* https://natlawreview.com

Reflections on 2019 in Technology Law, and a Peek into 2020

Article By:

Jeffrey D. Neuburger

It is that time of year when we look back to see what tech-law issues took up most of our time this year and look ahead to see what the emerging issues are for 2020.

Data: The Issues of the Year

Data presented a wide variety of challenging legal issues in 2019. Data is solidly entrenched as a key asset in our economy, and as a result, the issues around it demanded a significant level of attention.

- Clearly, privacy and data security-related data issues were dominant in 2019. The GDPR, CCPA and other privacy regulations garnered much consideration and resources, and with GDPR enforcement ongoing and CCPA enforcement right around the corner, the coming year will be an important one to watch. As data generation and collection technologies continued to evolve, privacy issues evolved as well. In 2019, we saw many novel issues involving mobile, biometric and connected car Facial recognition technology generated a fair amount of litigation, and presented concerns regarding the possibility of intrusive governmental surveillance (prompting some municipalities, such as San Francisco, to ban its use by government agencies).

- Because data has proven to be so valuable, innovators continue to develop new and sometimes controversial technological approaches to collecting data. The legal issues abound. For example, in the past year, we have been advising on the implications of an ongoing dispute between the City Attorney of Los Angeles and an app operator over geolocation data collection, as well as a settlement between the FTC and a personal email management service over access to "e-receipt" data. We have entertained multiple questions from clients about the unsettled legal terrain surrounding web scraping and have been closely following developments in this area, including the blockbuster *hiQ* Ninth Circuit ruling from earlier this year. As usual, the pace of technological innovation has outpaced the ability for the law to keep up.

- Data security is now regularly a boardroom and courtroom issue, with data breaches, phishing, ransomware attacks and identity theft (and cyberinsurance) the norm. Meanwhile, consumers are experiencing deeper and deeper "breach fatigue" with every breach notice they receive. While the U.S. government has not yet been able to put into place general

national data security legislation, states and certain regulators are acting to compel data collectors to take reasonable measures to protect consumer information (e.g., New York's newly-enacted SHIELD Act) and IoT device manufacturers to equip connected devices with certain security features appropriate to the nature and function of the devices secure (e.g., California's IoT security law, which becomes effective January 1, 2020). Class actions over data breaches and security lapses are filed regularly, with mixed results.

- Many organizations have focused on the opportunistic issues associated with new and emerging sources of data. They seek to use "big data" – either sourced externally or generated internally – to advance their operations. They are focused on understanding the sources of the data and their lawful rights to use such data. They are examining new revenue opportunities offered by the data, including the expansion of existing lines, the identification of customer trends or the creation of new businesses (including licensing anonymized data to others).

- Moreover, data was a key asset in many corporate transactions in 2019. Across the board in M&A, private equity, capital markets, finance and some real estate transactions, data was the subject of key deal points, sometimes intensive diligence, and often difficult negotiations. Consumer data has even become a national security issue, as the Committee on Foreign Investment in the United States (CFIUS), expanded under a 2018 law, began to scrutinize more and more technology deals involving foreign investment, including those involving sensitive personal data.

I am not going out on a limb in saying that 2020 and beyond promise many interesting developments in "big data," privacy and data security.

Social Media under Fire

Social media platforms experienced an interesting year. The power of the medium came into even clearer focus, and not necessarily in the most flattering light. In addition to privacy issues, fake news, hate speech, bullying, political interference, revenge porn, defamation and other problems came to light. Executives of the major platforms have been on the hot seat in Washington, and there is clearly bipartisan unease with the influence of social media in our society. Many believe that the status quo cannot continue. Social media platforms are working to build self-regulatory systems to address these thorny issues, but the work continues. Still, amidst the bluster and criticism, it remains to be seen whether the calls to "break up" the big tech companies will come to pass or whether Congress's ongoing debate of comprehensive data privacy reform will lead to legislation that would alter the basic practices of the major technology platforms (and in turn, many of the data collection and sharing done by today's businesses). We have been working with clients, advising them of their rights and obligations as platforms, as contributors to platforms, and in a number of other ways in which they may have a connection to such platforms or the content or advertising appearing on such platforms.

What does 2020 hold? Will Washington's withering criticism of the tech world translate into any tangible legislation or regulatory efforts? Will Section 230 of the Communications Decency Act – the law that underpins user generated content on social media and generally the availability of user generated content on the internet and apps – be curtailed? Will platforms be asked to accept more responsibility for third party content appearing on their services?

While these issues are playing out in the context of the largest social media platforms, any legislative solutions to these problems could in fact extend to others that do not have the same level of compliance resources available. Unless a legislative solution includes some type of "size of person" test or room to adapt technical safeguards to the nature and scope of a business's activities or sensitivity of the personal information collected, smaller providers could be shouldered with a difficult and potentially expensive compliance burden. Thus, it remains to see how the focus on social media and any attempt to solve the issues it presents may affect online communications more generally.

Quantum Leaps

Following the momentum of the passage of the National Quantum Initiative at the close of 2018, a significant level of resources has been invested into quantum computing in 2019. This bubble of activity culminated in Google announcing a major milestone in quantum computing. Interestingly, IBM suggests that it wasn't quite as significant as Google claimed. In any case, the development of quantum computing in the U.S. has progressed a great deal in 2019, and many organizations will continue to focus on it as a priority in 2020.

- Reports state that China has dedicated billions to build a Chinese national laboratory for quantum computing, among other related R&D products, a development that has gotten the attention of Congress and the Pentagon. This may be the beginning of the 21st century's great technological race.

- What is at stake? The implications are huge. It is expected that ultimately, quantum computers will be able to solve complex computations exponentially faster – as much as 100 million times faster — than classic computers. The opportunities this could present are staggering. As are the risks and dangers. For example, for all its benefits, the same technology could quickly crack the digital security that protects online banking and shopping and secure online communications.

- Many organizations are concerned about the advent of quantum computing. But given that it will be a reality in the future, what should you be thinking about now? While not a real threat for 2020 or the near-term thereafter, it would be wise to think about it if one is anticipating investing in long-term infrastructure solutions. Will quantum computing render the investment obsolete? Or, will quantum computing present a security threat to that infrastructure? It is not too early to think about these issues, and for example, technologists have been hard at work developing quantum-proof blockchain protocols. It would at least be prudent to understand the long-term roadmap of technology suppliers to see if they have even thought about quantum computing, and if so, to see to how they see quantum computing impacting their solutions and services.

Artificial Intelligence

We have seen significant level of deployment in the Artificial Intelligence/Machine Learning landscape this past year. According to the Artificial Intelligence Index Report 2019, AI adoption by organizations (of at least one function or business unit) is increasing globally. Many businesses across many industries are deploying some level of AI into their businesses. However, the same report notes that many companies employing AI solutions might not be taking steps to mitigate the risks from AI, beyond cybersecurity. We have advised clients on those risks, and in certain cases have been able to apportion exposure amongst multiple parties involved in the implementation. In

addition, we have also seen the beginning of regulation in AI, such as California's chatbot law, New York's recent passage of a law (S.2302) prohibiting consumer reporting agencies and lenders from using the credit scores of people in a consumer's social network to determine that individual's credit worthiness, or the efforts of a number of regulators to regulate the use of AI in hiring decisions.

We expect 2020 to be a year of increased adoption of AI, coupled with an increasing sense of apprehension about the technology. There is a growing concern that AI and related technologies will continue to be "weaponized" in the coming year, as the public and the government express concern over "deepfakes" (including the use of voice deepfakes of CEOs to commit fraud). And, of course, the warnings of people like Elon Musk and Bill Gates, as they discuss AI, cannot be ignored.

Blockchain

We have been very busy in 2019 helping clients learn about blockchain technologies, including issues related to smart contracts and cryptocurrency. 2019 was largely characterized by pilots, trials, tests and other limited applications of blockchain in enterprise and infrastructure applications as well as a significant level of activity in tokenization of assets, cryptocurrency investments, and the building of businesses related to the trading and custody of digital assets. Our blog, www.blockchainandthelaw.io keeps readers abreast of key new developments and we hope our readers have found our published articles on blockchain and smart contracts helpful.

Looking ahead to 2020, regulators such as the SEC, FinCEN, IRS and CFTC are still watching the cryptocurrency space closely. Gone are the days of ill-fated "initial coin offerings" and today, security token offerings, made in compliance with the securities laws, are increasingly common. Regulators are beginning to be more receptive to cryptocurrency, as exemplified by the New York State Department of Financial Services revisiting of the oft-maligned "bitlicense" requirement in New York.

Beyond virtual currency, I believe some of the most exciting developments of blockchain solutions in 2020 will be in supply chain management and other infrastructure uses of blockchain. 2019 was characterized by experimentation and trial. We have seen many successes and some slower starts. In 2020, we expect to see an increase in adoption. Of course, the challenge for businesses is to really understand whether blockchain is an appropriate solution for the particular need. Contrary to some of the hype out there, blockchain is not the right fit for every technology need, and there are many circumstances where a traditional client-server model is the preferred approach. For help in evaluating whether blockchain is in fact a potential fit for a technology need, this article may be helpful.

Other 2020 Developments

Interestingly, one of the companies that has served as a form of leading indicator in the adoption of emerging technologies is Walmart. Walmart was one of the first major companies to embrace supply use of blockchain, so what is Walmart looking at for 2020? A recent *Wall Street Journal* article discusses its interest and investment in 5G communications and edge computing. We too have been assisting clients in those areas, and expect them to be active areas of activity in 2020.

Edge computing, which is related to "fog" computing, which is, in turn, related to cloud computing, is simply put, the idea of storing and processing information at the point of capture, rather than communicating that information to the cloud or a central data processing location for storage and processing. According to the WSJ article, Walmart plans on building edge computing capability for other businesses to hire (following to some degree Amazon's model for AWS). The article also talks

about Walmart's interest in 5G technology, which would work hand-in-hand with its edge computing network.

Our experience with clients suggest that Walmart may be onto something. Edge and fog computing, 5G and the growth of the "Internet of Things" are converging and will offer the ability for businesses to be faster, cheaper and more profitable. Of course this convergence also will tie back to the issues we discussed earlier, such as data, privacy and data security, artificial intelligence and machine learning. In general, this convergence will increase even more the technical abilities to process and use data (which would conceivably require regulation that would feature privacy and data security protections that are consumer-friendly, yet balanced so they do not stifle the economic and technological benefits of 5G).

This past year has presented a host of fascinating technology-based legal issues, and 2020 promises to hold more of the same. We will continue to keep you posted!

We hope you had a good 2019, and we want to wish all of our readers a very happy and safe holiday season and a great New Year!

National Law Review, Volume IX, Number 357