Proskauer

Reflections on the TechLaw Issues of 2018…and a Look Forward. Will 2019 Be a Year on the Edge, in the Fog, or Maybe Just in the Cloud?

New Media and Technology Law Blog on **December 21, 2018**

Yes, it's time for the end-of-year blog post – a look back at interesting issues of 2018 and a look forward to what we see coming down the pike in the new year.

The Look Back

- In the past year, blockchain buzz was everywhere. Although still early, blockchain has in fact began to show promise as a technology bringing efficiency and cost reduction to many business operations. In 2018, many industries tested the technology and started pilot programs with an eye to replacing or supplementing traditional client-server systems with a distributed ledger-based system. 2019 promises much more in the adoption of blockchain. For continuing coverage of some of the more novel issues that blockchain presents, subscribe to our *Blockchain and the Law blog*.
- "Web scraping" (also known as spidering and crawling) remained at the forefront in 2018 as companies used scraping for purposes such as consumer-facing data aggregation, real-time e-commerce analytics (e.g., dynamic pricing strategies), competitive intelligence, user sentiment analysis, etc. 2018 produced many important scraping decisions in the courts, including those about CFAA liability and the intersection of scraping and software licensing, and we await the Ninth Circuit's decision in the closely-watched *hiQ appeal*, which will hopefully address a number of important open issues presented by the practice.
- Privacy and data security continued to be a hot-button boardroom issue this year. The GDPR became effective, and California passed major privacy legislation which will take effect in 2020. The almost daily announcement of data security breaches continues to spawn class action litigation, testing the principles of standing after *Spokeo*. The federal government has pushed multiple initiatives to improve the nation's cyber defenses. The wave of litigation under the Illinois biometric privacy law (BIPA) against Illinois employers and businesses persisted in 2018, and the continued viability of such suits may hinge on an upcoming ruling by the Illinois Supreme Court, as well as the outcome in California courts regarding the BIPA

actions against social media entities. See our Privacy Law Blog for more discussion on 2018 privacy and data security developments.

The Look Ahead

So what does 2019 hold? Well, we expect to see many of the 2018 developments continue to impact us in 2019. Beyond these issues, what else might crop up in 2019?

Quantum Computing

Quantum computing is here. While conventional computers use binary data or bits (i.e., Os and 1s) to store and process information (a bit can either store a 0 or 1), a quantum computer uses quantum bits or "qubits," which can be in what's called the superposition of zero and one at the same time (e.g., a qubit can store a 0, 1, or a summation of both 0 and 1). Ultimately, it is expected that quantum computers will solve complex computations exponentially faster – as much as 100 million times faster — than classic computers. Quantum computers are a reality today and more development will emerge in the coming year.

Quantum computing presents many issues and risks. Current encryption and cryptography systems are premised on the assumption that there are limits to the resources and processing power that can be brought to breaking such systems. Quantum computers may be powerful enough (perhaps) to break the public key cryptography systems currently in use that protects secure online communications and encrypted data (or not). Clearly, basic password protection would appear quaint in light of the resources quantum computing could bring to a "brute force" hack. China reportedly has a head start in quantum encryption technologies to produce secure communications networks, among other things. In response, as December drew to a close, both the House and Senate passed a bipartisan bill (H.R. 6227) that directs the President to implement a National Quantum Initiative Program to establish an advisory committee, national goals and a long-term R&D plan for quantum technology applications. As of this writing, the bill is expected to reach the President's desk and be signed.

We have been working with clients in responding to the phenomenon of quantum computing. How can such computing power be put to use in business? What are the risks? How should security systems be modified to address it? How does quantum computing impact blockchain? What are the ethical issues associated with the use of quantum computing? These questions and more will be addressed in the coming year.

Edge and Fog Computing

By now, most tech lawyers have at least some sense of such concepts as “cloud computing” and “SaaS.” Well, things are about to get a little more complicated. The volume of the “digital exhaust” of our lives — the terabytes of data that are created every single day from our computers, our phones, our cars, our refrigerators, our thermostats, our digital helpers, and all of the IoT devices and sensors — is overwhelming. Of course, the cloud seems like the instinctive solution for the storage of such data, as one of the characteristics that makes the cloud attractive is that it is flexible and seems to have limitless expansion capacity to accommodate the storage of such data at a relatively low cost. However, should all of that data be stored on the cloud? Is that the right way to treat all data, or should different types of data be treated differently? Are there special needs for some types of data with respect to latency, data security and availability?

Cloud computing is, of course, very popular and has experienced widespread general adoption. However, cloud computing is not the perfect solution for situations where milliseconds of latency matter. Cloud computing involves the transmission of data from the data source to the “cloud” – usually a remote data center — and then to other computer systems as the data is processed. This can involve among other issues, potential delays in transmission.

Thus, the emergence of edge and fog computing.

Edge computing (or the “near cloud”) refers to the processing of data that occurs within the collecting device itself or close to the location of the data collection or generation, as opposed to having the collected data sent to a faraway data center for processing. Edge computing allows for the collection, processing and storage of data at the site of collection of the data, such as at a factory where sensors might be able to process data and analyze it in real time without the latency that can come from beaming the data back and forth.

OK, so that is edge computing, but what does that have to do with fog? While edge computing is mainly focused on running specific applications among a limited network of sensors and transmitting data to the main network when appropriate, fog computing is a multi-layer architecture at the local area network level (often referred to as a “fog node”), between the edge (where data is collected) and the ultimate network (e.g., cloud provider, company’s data centers). Fog computing serves as an intermediate step in the processing or aggregating of data from multiple “edge” locations before storage.

Such technologies are already at play in such things as self-driving cars (where reducing processing time by milliseconds can be critical), smartphones and wearables, smart city and smart building applications, and content delivery networks. They will soon be applied for additional uses, including enhancing premises security, monitoring environmental conditions in the supply chain or on a farm, improving the capabilities of existing smart devices, innovating wearable health devices and telemedicine, and crunching retail sales data at the store level Sometimes coupled with developments in blockchain, fog and edge computing can be attractive t organizations looking to lower costs (lessen bandwidth and power needs, lower network traffic), improve performance by reducing latency, mitigate the risk of telecom failures, and allow for the distributed use and analysis of data in offline environments (or areas of limited connectivity).

So we have started to spend a lot of time on the edge, fog and cloud computing. [What is with the tech industry’s fascination with atmospheric metaphors anyway?] We are finding that the early transactions involving these technologies have raised interesting twists on the usual tech-related legal issues. For example, who is responsible for maintaining these devices and networks and addressing fixes to newly discovered vulnerabilities? Who has liability for technology failures? What are the privacy and data security implications? How does the doctrine of force majeure apply? Can the use of fog and edge computing alleviate some of the legal concerns regarding data localization and transfer issues? We have begun to advise clients and negotiate these issues and 2019 promises to bring more of these issues to the forefront.

In closing, 2018 was another fascinating year, and 2019 will likely be equally as dynamic. We look forward to working with all of our friends on these important issues in the coming year.

In the meantime, we want to wish all of our readers a very happy and safe holiday season and a great New Year!

View Original

Related Professionals

- **Jeffrey D. Neuburger**