Message from the Chair

Dear Cyberspace Colleagues:

I am very excited about the strong lineup of CLE programs the Cyberspace Law Committee has for Annual Meeting in just two months. They are:

- "Autonomous Car Crashes - Who or What Dunnit? Will IP and Cybersecurity Lawyers Replace PI Lawyers in Sorting Out the Legal Issues?" - jointly sponsored with IP Committee
- "Cyber Extortion: The Ethics of Advising on Ransom Demands to Restore Client Digital Assets"
- "GDPR: Blueprint for a New World Order?" - jointly sponsored with Consumer Financial Services Committee
- "Legal Ethics and Cryptocurrency"
- "What Business Lawyers Need to Know about Blockchain, Smart Contracts, and ICOs from Fundamentals to Transformative Applications"

The programs will include 4 hours of professional responsibility credit and the latest info on significant developments that seem to be happening daily. See below for more information.

As part of our Cyberspace Law Committee meeting, we also will have a presentation by the person charged with leading a team to implement our host city's initiative to use smart mobility technologies and data analytics to reduce congestion and improve transportation reliability, access, and safety. We will explore "Smart Mobility: Can Data Analytics Solve Our Transportation Woes (Without Ruining Our Private Life?)"

If you have been procrastinating about registering, I strongly encourage you to register now. The Fairmont Austin (our base hotel) was just about sold out as of this writing! You must register for the meeting first to book at the group rate at the Fairmont. Hotel reservations made without a corresponding paid meeting registration may be cancelled.

We also have planned a fabulous dinner on Thursday evening at Second Bar + Kitchen. With some generous sponsorship by StoneTurn and SaGo, our dinner will be both delicious and very reasonably priced. Details will be posted in a few days!

Keep in mind that you have many opportunities to share your expertise in ways big and small and get published while doing so. Please consider submitting a short summary of a current legal issue or a longer article for Business Law Today. If you would like some guidance, please contact our Content Director Juliet Morigiello or Current Law Task Force Chair Mike Silvestro.

We also are looking for another Membership Director for our committee. Let me know if you might be interested in that opportunity or have other ideas about how you would like to get involved with the committee's work!

Regards,

Cheryl Dancey Balough
Chair, Cyberspace Law Committee
Annual Meeting CLE Programs

As mentioned, we have an exciting lineup of CLE programs slated for the Annual Meeting. Read below and whet your Cyberlaw appetite:

Autonomous Car Crashes - Who or What Dunnit? Will IP and Cybersecurity Lawyers Replace PI Lawyers in Sorting Out the Legal Issues?"

A modern day who or what dunnit for autonomous vehicle crashes will be investigated during a joint Cyberspace Law and Intellectual Property program at the September annual meeting in Austin. The panel brings together auto industry, regulatory, cybersecurity, and intellectual property attorneys to discuss liability issues relating to autonomous vehicles when they crash, such as should the manufacturer or software designer be responsible? The panel also will explore the question: will IP and cybersecurity lawyers replace PI lawyers in sorting out the legal issues? Co-chairs of the program are the Hon. Lucy Koh, U.S. District Court Judge for the Northern District of California, and Peter Snell, Partner, Gowling WLG.

What Business Lawyers Need to Know About Blockchain, Intelligent Contracts and ICOs, from Fundamentals to Transformative Applications.

As the disruptive potential of blockchain and smart contracts expands, counsel are increasingly called on to understand distributed ledger technology (DLT), and to advise clients across sectors regarding its legal implications. Through the diverse perspectives of practitioners, platform providers, pioneering users of blockchain, and other experts, the panel will explore a range of exciting and novel applications of DLT and smart contracts. The program will explain the technical and legal fundamentals of blockchain technology and intelligent contracts, beginning with an overview of the common nomenclature that business lawyers should understand, before delving into several transformative use cases. Panelists will discuss razor's edge legal issues around, and uses of, the technology including legal document creation, execution, access, and storage; crypto offerings and ICOs; privacy and security considerations; and statute of frauds, UETA, the ESIGN Act, and other applicable laws and regulations.

Legal Ethics and Cryptocurrency

The chairmen of the SEC and CFTC have recently expressed concerns that the legal advice some counsel have provided to entities operating in the cryptocurrency space elevates "form over substance" and has contributed to fraudulent and illegal activity. This panel will discuss the ethical issues surrounding providing legal counsel to cryptocurrency businesses and will offer practical advice on how appropriately to serve clients whose business models may be ahead of the law. The panel will also explore other ethical issues associated with cryptocurrency, including the Nebraska ethics opinion regarding lawyers accepting payment of fees in bitcoin and the Office of Government Ethics guidance on federal employees' obligations to disclose holdings of cryptocurrency. The panel will also discuss the July 2nd SEC settlement with an attorney and his law firm's business manager regarding illegal sales of UBI Blockchain Internet Stock.

Our panelists include:

- David Hirsch, Senior Counsel and Cyber Liaison, Securities and Exchange Commission (Fort Worth, TX)
- Prof. Donna Nagy, C. Ben Dutton Professor of Law, Indiana University Maurer School of Law (Bloomington, IN)
- Stephen D. Palley, Partner, Anderson Kill (Washington, DC)
David Hirsch is an enforcement attorney at the SEC where he has worked on a number of the Commission's investigations related to cryptocurrency and initial coin offerings, including the prosecution of AriseBank. Prof. Nagy teaches and writes extensively in the areas of securities law, ethics and financial disclosure requirements. In 2011 she testified before Congress on legislation that become the STOCK Act. Stephen Palley is in private practice and represents clients in the cryptocurrency and blockchain space.

Subcommittee News

From the Current Law Task Force

Current Law Task Force Meeting - July 11

Are you interested in writing about emerging topics in cyberspace law? Would you like to publish a piece on a recent development, but don't have the time to draft a long article? Are you looking for a way to get more involved with the Cyberspace Law Committee without traveling to a meeting?

If so, call in to the next meeting of the Cyberspace Law Committee's Current Law Task Force on July 11 at 10:30 am CT/11:30 am ET. New members are always welcome.

The Current Law Task Force tracks and reports on recent developments in cyberspace law and serves as an incubator for publications and presentations. There are a variety of available publication opportunities, including contributions to the Cyberspace Law Committee Newsletter and Business Law Today. The Task Force can help you publish works of varying length and detail, ranging from long-form articles to pieces as brief as one paragraph.

The Current Law Task Force meets through monthly conference calls to discuss new developments and ideas for publications. The dial-in information for the call is below:

Call In: 312-667-9356
Conference ID: 079455
Security Pin: 160049

Brazil's GDPR was approved at the House of Representatives

Caio Lima, Opice Blum

On May 29th, the Brazilian Bill on Data Protection (which is being called as the "Brazil's GDPR") was approved by the House of Representatives in what represents a step closer to a more comprehensive data protection law in Brazil. It is clear that the GDPR heavily influenced this bill.

Brazil does not have an omnibus data protection law yet. Data protection is regulated by the Federal Constitution, the Defense Code, the Civil Code, and sectoral laws, such as the Civil Rights Framework for the Internet ("Marco Civil da Internet") and the Credit Reports Law ("Lei do Cadastro Positivo"). So, in our opinion that bill is important, mainly because it will enhance the level of trustworthiness of companies, making it easier for them to see Brazil as a safe place to invest money.

It is important to highlight that this bill will also be applicable to companies headquartered outside of Brazil provided that they treat (i.e., collect, share, use,
or host, among others) data of data subjects inside of Brazil or that they offer goods or services for data subjects physically located in Brazil. Note that this is a territorial criteria, and, as a result, citizenship will not be a relevant consideration.

After the approval at the lower house, the bill was sent to Senate, where it arrived on early June. Now it is going to be analyzed by senatorial internal commissions. If those commissions approve the bill, it may be brought up for vote by Senators. If Senators change something in the bill, then the approved text at Senate will need to have a final vote at the lower court. If no change is made at Senate, then the law can be sent directly for the Presidential sanction, who can sanction it totally or partially. If unchanged, the law would come into force 18 months after being enacted.

The California Consumer Privacy Act of 2018 (CaCPA) - Key Provisions and Concepts

Michael Silvestro, Skarzynski Black LLC

On June 28, Gov. Jerry Brown signed the California Consumer Privacy Act of 2018 ("CaCPA"), a landmark privacy law that shares some features of the GDPR. CaCPA represents a sea change in US data privacy law and adds yet another layer to the complex patchwork of data privacy laws and regulations.

The sweeping scope of CaCPA is evident from its preamble alone, which explicitly states its intent to “further Californians’ right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights: (1) The right of Californians to know what personal information is being collected about them. (2) The right of Californians to know whether their personal information is sold or disclosed and to whom. (3) The right of Californians to say no to the sale of personal information. (4) The right of Californians to access their personal information. (5) The right of Californians to equal service and price, even if they exercise their privacy rights.

Read more...

Committee Member News

Sarah Jane Hughes was an invited speaker at the Federal Trade Commission's symposium "Decrypting Cryptocurrency Scams" held in Chicago on June 25th. Her panel included representatives from the SEC and CFTC. Andrew Smith (current chair of the Consumer Financial Services Committee and newly installed Director of the FTC's Bureau of Consumer Protection) gave the opening remarks at the symposium.

On June 19, 2018 Lisa R. Lifshitz, co-Chair of the Robotics and Artificial Intelligence Subcommittee, was presented the Zenith Award by Lexpert/Thomson Reuters for Mid-Career Excellence in Computer and IT Law in Toronto.

Call for Future Contributions

Do you have something that might make a good contribution to next month's Cyberspace Law newsletter? Email Tom Kierner with your blurb! Have a less Cyberspace-y contribution? It might be a good fit for Business Law Today. Email Juliet Moringiello, and she will help you with the submission process.
On June 28, Gov. Jerry Brown signed the California Consumer Privacy Act of 2018 (“CaCPA”), a landmark privacy law that shares some features of the GDPR. CaCPA represents a sea change in US data privacy law and adds yet another layer to the complex patchwork of data privacy laws and regulations.

The sweeping scope of CaCPA is evident from its preamble alone, which explicitly states its intent to “further Californians’ right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights: (1) The right of Californians to know what personal information is being collected about them. (2) The right of Californians to know whether their personal information is sold or disclosed and to whom. (3) The right of Californians to say no to the sale of personal information. (4) The right of Californians to access their personal information. (5) The right of Californians to equal service and price, even if they exercise their privacy rights.”

CaCPA also presents additional compliance mandates, including specific notice provisions and mechanisms for allowing consumer requests, that will likely require covered businesses to revise privacy notices and policies. In addition, CaCPA creates private consumer causes of action and provides for civil actions and enforcement by California’s Attorney General.

This article will highlight some of the key provisions of CaCPA, which takes effect January 1, 2020 (subject to anticipated amendments). The full text of CaCPA is available for further reading at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

Covered Entities and Consumers
CaCPA limits covered “consumers” to legal residents of California as defined by 18 C.C.R. § 17014. Non-residents who are temporarily visiting California for work or pleasure are not likely to be covered.

Notably, additional protections are provided for certain minor consumers, including an opt-in requirement for the sale of a minor’s personal data. Under Section 1798.120(d), businesses are prohibited from selling personal information of consumers if the business has “actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer’s parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer’s personal information.”

CaCPA applies to entities “doing business” in California that collect consumer personal information concerning consumers (i.e., California residents) that, alone or jointly with others, determines the means and purposes of processing such personal information and meets one of the following criteria:

(1) has annual gross revenues in excess of $25 million dollars; or
(2) buys, receives, sells or shares, alone or in combination, the personal information of 50,000 or more “consumers, households, or devices” for commercial purposes; or
(3) derives 50% or more of its annual revenue from selling consumer personal information.

For businesses without a physical presence in California, under Section 1798.45 (a)(6) certain commercial activities may be exempted if the “commercial conduct takes place wholly outside of California.” This may be difficult to establish, however, as it would require: (1) collection while the consumer was outside of California; (2) no part of the sale of the consumer’s personal information occurred in California; and (3) no personal information collected while the consumer was in California is sold.

“Personal Information” Is Broadly Defined
“Personal information” is more broadly defined under CaCPA than many other privacy laws, including the GDPR. Under CaCPRA, “personal information” means: “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” “Personal Information” under CaCPA also includes information about households and certain derivatives of collected data, such as consumer profiles, which may be broader than personal information under the GDPR and other privacy laws. Examples of “personal information” under CaCPA include, but are not limited to: real names, aliases, postal addresses, unique personal identifiers, IP addresses, account names, social security numbers, driver’s license numbers, passport numbers; biometric information; commercial information, including records of items or services purchased or considered or “other purchasing or consuming histories or tendencies;” geolocation data; “audio, electronic, visual, thermal, olfactory, or similar information;” professional or employment related information; and education information not defined as publicly available personally identifiable information under FERPA.

The definition of “personal information” explicitly includes certain consumer profiling derived from such information, including “[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.”

Certain personal information regulated under HIPPA, FCRA, CMIA, GLBA and the Driver’s Privacy Protection Act may be exempted from CaCPA.

Consumer Right to Request Access to or Details Concerning Collected Personal Information
Under CaCPA, consumers have various rights to access and restrict the use of their personal information. Businesses are obligated to respond to consumer inquiries following receipt of a “verifiable request.” As such, covered businesses will need to “reasonably verify” that requests are made by the consumer or other person “authorized by the consumer to act on such consumer’s behalf” in accordance with California law.

Notably, businesses are prohibited from requiring consumers to create an account with the business in order to submit a verifiable request or opt out of the sale of personal information. Consumers covered under CaCPA have the right to request that “a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.” Responses to consumer information requests must be made within 45 days, and businesses are required to disclose the information free of
charge, but not more than twice in a 12-month period. Certain information collected for single one-time transactions may be exempted.

Among the information that must be disclosed upon request are:
(1) the categories of personal information collected;
(2) categories of sources from which persona information is collected;
(3) the business or commercial purpose for collecting or selling personal information;
(4) categories of third parties with whom the business shares personal information; and
(5) the “specific pieces” of personal information the business has collected about that consumer.

**Consumer Right to Delete Personal Information**
Under CaCPA, cosumers also have the “right to request that a business delete any personal information about the consumer which the business has collected from the consumer.” This extends to personal information held by service providers who have received the personal information from the collecting party.

There are several exceptions under which businesses are not required to delete personal data, however, including compliance with legal obligations and continued internal uses “in a lawful manner that is compatible with the context in which the consumer provided the information.”

**Consumer Right to Opt Out of the Sale of Personal Information**
CaCPA also provides consumers with “the right to opt out” of the sale of their personal information. At any time, consumers can direct a business that sells personal information about the consumer to third parties not to sell that consumer’s personal information. Among other requirements, businesses that sell consumer personal information to third parties must provide notice of the potential sale of personal information and the right to opt out of the sale of that information to third parties.

As noted above, for certain minors, sale of personal information requires the consumer (or their guardian) to opt-in. In addition, for consumers that have opted out of the sale of personal information, businesses must wait at least 12 months before asking that consumer to authorize that sale of the consumer’s personal information.

**Consumer Right to Equal Treatment**
Covered businesses are also prevented from discriminating against consumers due to the exercise of any rights under CaCPA. Under Section 1798.125, prohibited practices include denying goods or services, charging different prices or rates for goods or services, or suggesting that consumers will receive a difference price, rate, or quality of goods or services based upon a consumer’s exercise of any CaCPA rights.

**Notice to Consumers**
CaCPA also contains a number of notice-related provisions that will prompt many businesses to review and revise their privacy notices and policies. Among them, covered businesses must provide two or more methods for submitting information requests, including a toll-free telephone number and web site (if the business has a web site).
Covered businesses may also be required to display “clear and conspicuous link” on the businesses’ homepage titled “Do Not Sell My Personal Information” that allows consumers to opt out of the sale of personal information. Links to the businesses’ online privacy policies or any “California-specific description of consumers’ privacy rights” may also be required.

**Attorney General Enforcement and Private Cause of Action**
Importantly, CaCPA also provides for a private consumer cause of action if that consumer’s nonencrypted or nonredacted personal information is “subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.” Statutory damages are provided in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater. Injunctive and declaratory relief are also statutorily available.

In addition, California’s Attorney General may bring civil actions on behalf of California residents. For intentional violations, civil penalties may be as high as $7,500 per violation. Businesses may also solicit compliance advisory opinions from the Attorney General.

**Concluding Thoughts**
Taken in whole, the CaCPA represents a significant change in US data privacy law and warrants careful review by potentially covered businesses and their counsel. Although it is likely that CaCPA may be amended before it takes effect in 2020, its passage underscores the need for potentially covered businesses to develop robust privacy, security and compliance programs. Moreover, CaCPA is also likely to apply to a large number of domestic businesses that were not subject to the GDPR but do business with California residents or their data.