Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | October 2019

The California Consumer Privacy Act continues to be in the headlines as its January 1, 2020 effective date approaches. The Governor just signed several amendments passed at the end of the legislative session, and the state Attorney General released draft regulations on a number of important parts of the law, bearing directly on companies' compliance obligations. In our first **article**, Joan Stewart and Kat Scott discuss the implications of these latest developments. We will also host a **webinar** on November 7 that will go into greater detail on these developments and provide practical compliance tips.

In this issue, we also discuss two other important data governance issues for businesses. First, we analyze the legal uncertainty for companies around trans-Atlantic data transfers, given recent court challenges, in an **article** by Joan Stewart, Kamila Benzina, and Stephen Conley. Next, I **discuss** the FTC's push to hold companies liable for a range of third parties' activities, including compliance with privacy laws. The **"In Brief"** section also provides a further update on our commentary on political privacy.

Feel free to reach out to me or any of the other authors with feedback or questions. I can be reached at 202.719.4533 or dpozza@wileyrein.com. Thank you as always for reading.

-Duane Pozza, Partner, Privacy, Cyber & Data Governance Practice

California Consumer Privacy Act Update – Governor Signs Final Amendments (for This Year) and AG Releases Draft Regulations

By Joan Stewart and Kathleen E. Scott

Governor Signs Final Amendments Prior to January 1, 2020 Effective Date

The California legislature passed several amendments to the California Consumer Privacy Act (CCPA) at the end of this year's session: AB 25, AB 874, AB 1146, AB 1355, and AB 1564. On October 11, 2019, the Governor approved them all.

Several of the amendments include common-sense limitations on certain CCPA obligations. Two amendments, in particular, work to limit the CCPA's scope.

- ***First***, AB 25 excludes from most CCPA coverage personal information of a business's job applicants, employees, and others similarly situated. Specifically, AB 25 exempts information "collected from a

IN THIS ISSUE:

continued on page 2

Continued from 1

natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor [defined to require a written contract] of the business." Importantly, this amendment does not remove certain notice rights of job applicants, employees, and others, and does not remove these individuals' rights to pursue a private right of action against a business if their personal information is breached. This provision will sunset after one year, meaning that unless it is extended, job applicants, employees, and others covered by this amendment will be treated like any other consumer under the law, with all corresponding rights.

- ***Second***, AB 1355 exempts certain B2B information from certain CCPA consumer rights. Specifically, AB 1355 provides a one-year exemption, from several but not all CCPA provisions, for "personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency." As with AB 25, unless extended, this exemption will sunset in one year and does not remove an individual's right to pursue a private right of action if their information is compromised in a breach.

Additionally, some amendments refine the definition of personal data. AB 874 adds a reasonableness qualification, redefining personal information as "information that ... is **reasonably capable** of being associated with ... a particular consumer or household." AB 1355 – in addition to its B2B exemption – further clarifies the definition of personal information to confirm that deidentified or aggregate consumer information is excluded.

The legislature also clarified the obligations of a business that sells goods only via a website. Specifically, AB 1564 provides that businesses that both operate exclusively online and have a direct relationship with the consumer are only required to provide one method to submitting requests for exercise of consumer rights, and that method can be an email address. Thus, this amendment removes the requirement to maintain a toll-free number for non-brick-and-mortar businesses.

Beyond CCPA amendments, the legislature adopted an amendment to California's data breach law that works to expand the risk of liability under the CCPA. Specifically, AB 1130 revises the definition of "personal information" in the California data breach law to include unique biometric data such as "a fingerprint, retina, or iris image, used to authenticate a specific individual," as well as other data elements, including tax identification numbers, passport numbers, military identification numbers, or other unique identification numbers (e.g., driver's license numbers or California identification card numbers). Given the fact that the CCPA's private right of action for data breaches is tied to the definition of "personal information" in this law, this expansion expands the scope of the CCPA's private right of action.

With the legislative session closed for the year, there will be no further amendments to the law before it takes effect on January 1, 2020.

AG Releases Draft Regulations

On October 10, 2019, California Attorney General (AG) Xavier Becerra released the long-awaited draft

continued on page 3

California Consumer Privacy Act Update – Governor Signs Final Amendments (for This Year) and AG Releases Draft Regulations

Continued from 2

regulations for CCPA. These rules, once finalized, will govern compliance with the CCPA.

The proposed regulations establish procedures and provide guidance for businesses covered under the CCPA. The draft regulations cover a lot of ground. For example, the proposed regulations detail what notice must be provided at the time of data collection – distinguishing between online and offline (in person) collection. They also outline the notice that must be provided to consumers about how to exercise an opt-out request. For those businesses offering financial incentives or price of service differences, a description of the specific notice that must be provided about those offerings is also detailed in the draft. The draft regulations also detail requirements related to privacy policies, business practices for handling consumer requests, verification procedures, training, record-keeping, and minors.

The release sets into motion a series of events and deadlines in the formal rulemaking process, through which interested stakeholders will have multiple opportunities to engage. Specifically, the AG plans to hold four public hearings, where interested parties can present oral or written testimony. Those hearings are scheduled for December 2 in Sacramento, December 3 in Los Angeles, December 4 in San Francisco, and December 5 in Fresno. Additionally, the Attorney General will accept written comments until December 6. ■

For more information on the draft regulations and how your business can engage in the rulemaking process, see our recent **Client Alert**, tune in to our **upcoming webinar,** or contact:

Joan Stewart
202.719.7438 | jstewart@wileyrein.com

Kathleen E. Scott
202.719.7577 | kscott@wileyrein.com

CALIFORNIA CONSUMER PRIVACY ACT: LATEST DEVELOPMENTS AND COMPLIANCE STRATEGIES

WEBINAR | November 7, 2019 @ 2:00 pm – 3:00 pm ET

Join us to discuss how businesses will be affected by the latest developments with the California Consumer Privacy Act — including recent legislative amendments and draft regulations issued in October. We will discuss practical tips to operationalize CCPA compliance as the law's January 1, 2020 effective date approaches, and what businesses need to know about the California Attorney General's ongoing rulemaking proceedings.

Duane C. Pozza
Partner
dpozza@wileyrein.com
202.719.4533

Antonio J. Reynolds
Partner
areynolds@wileyrein.com
202.719.4603

Joan Stewart
Of Counsel
jstewart@wileyrein.com
202.719.7438

Kathleen E. Scott
Associate
kscott@wileyrein.com
202.719.7577

Companies Engaged in Trans-Atlantic Data Transfers Face Legal Uncertainty

By Joan Stewart

Kamila Benzina and Stephen Conley, who are Wiley Rein law clerks, co-authored this article with Ms. Stewart.

Many U.S. companies that are engaged in trans-Atlantic data transfers rely on either standard contractual clauses (SCCs) or the U.S.-EU Privacy Shield Framework to comply with data transfer requirements under the European Union's comprehensive privacy law, the General Data Protection Regulation (GDPR).[1] Recent court challenges to the "adequacy" of these data transfer mechanisms have left U.S. businesses with mounting legal uncertainty as to the future legitimacy of these long-standing data transfer practices.

Two cases before the Court of Justice of the European Union (CJEU) threaten SCCs and the Privacy Shield Framework and could require companies to develop alternative methods to comply with GDPR cross-border transfer requirements. In *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (C-311/18), privacy activist Maximillian Schrems – the same plaintiff whose case brought down the Safe Harbor agreement in 2015 – is challenging SCCs used by Facebook.[2] If successful, this case could compromise the viability of SCCs worldwide. In a separate case, *Quadrature du Net v. Commission* (T-738/16), three French NGOs[3] are challenging the Privacy Shield Framework, claiming that it currently violates EU fundamental rights by failing to curb surveillance abuses by the U.S. government.[4]

Privacy Shield and SCC Background

The GDPR generally prohibits cross-border transfers of data unless (1) the European Commission has granted the recipient country an "adequacy decision," meaning the Commission determined the country offers an adequate level of data protection; (2) the controller or processor of the data provides appropriate safeguards; or (3) the cross-border data transfer is justified under one of the enumerated derogations.[5]

The European Union granted the U.S. a qualified adequacy decision that applies only to companies who comply with the voluntary Privacy Shield Framework.[6] The Privacy Shield Framework went into effect on August 1, 2016, replacing the 15-year-old Safe Harbor framework. The updated Framework includes stricter obligations related to data retention and cross-border transfers, more rigorous documentation and monitoring, and a prominent role for national data protection authorities in the investigation of claims.[7] Under the Privacy Shield, participating organizations self-certify to the U.S. Department of Commerce (DOC) that they will comply with the 23 privacy principles laid out in the agreement, including the principles of notice, choice, accountability, security, and data integrity.[8] Participating companies must also provide appropriate remedies for EU data subjects whose data rights have been violated under the agreement.[9] Compliance by participating companies is monitored and enforced by both the DOC and the Federal Trade Commission (FTC).[10]

While participation in the Privacy Shield Framework is increasing, the most widely used data transfer mechanism is SCCs, which are contracts entered into by senders and receivers of cross-border data that bind parties to standardized data protection clauses.[11] Companies may submit clauses to the Data Protection Authority (DPA) for approval, or choose to use the applicable model clauses that have been issued by the EU. The EU has issued three sets of model clauses for data transfers – two for transfers from EU data *controllers* to non-EU data *controllers*, and one for transfers from EU data *controllers* to non-EU data *processors*. [12]

There are other avenues for companies to bring their cross-border data practices into compliance, but most are far more costly and time-consuming than the two described above. For example, Article 46 of

continued on page 5

Continued from 4

the GDPR allows for companies to establish Binding Corporate Rules (BCR), which serve as internal codes of conduct regulating the internal transfer of personal data between members of a corporate group. BCRs must be approved by an EU Data Protection Authority, which involves a time-consuming and expensive approval process that typically is viable only for large multinational companies.

In the absence of an adequacy decision or appropriate safeguard, cross-border data transfer may occur if a derogation, or exception, applies. The derogations listed in the GDPR are fact-specific and include situations where the data subject has explicitly consented to the data transfer or the transfer is necessary for public interest reasons, among others.[13] While derogations apply on a case-by-case basis, they alone are likely not adequate to serve as a company's primary data transfer mechanism.

Schrems II and Quadrature du Net

The legal standing of both the Privacy Shield and SCCs remain in doubt as the CJEU considers challenges to both mechanisms.

In *Facebook Ireland & Schrems,* nicknamed *Schrems II,* privacy activist Maximillian Schrems is challenging the legality of SCCs used by Facebook, claiming that Europeans' data cannot be sufficiently protected under American surveillance laws. The case was initially brought by Schrems before the Irish Data Protection Commissioner in 2015 against Facebook and transferred to the Irish courts.[14] On October 3, 2017, the Irish High Court found that U.S. surveillance acting under the authority of Section 702 of the Foreign Intelligence Surveillance Act (FISA) had engaged in "mass indiscriminate processing" of Europeans' data.[15]

The question now before the CJEU is whether surveillance under FISA breaks European data protection laws and necessitates stronger protections than those provided under SCCs.[16] Schrems' argument is that Facebook is required to assist the U.S. government in surveillance of non-civilians, and thus the SCCs that facilitate this should be invalidated.[17] The Irish Data Protection Commissioner, however, believes that the Privacy Shield should also contemporaneously be considered by the CJEU, which is at odds with the European Commission's position that only SCCs should be adjudicated.[18] The eleven questions on review are expected to be decided by early 2020, with a nonbinding opinion issued on December 12, 2019 by the CJEU Advocate General.[19]

The validity of the Privacy Shield Framework will be considered by the CJEU in *Quadrature du Net v. Commission*, where French privacy groups argue that, like the Safe Harbor agreement, the Privacy Shield fails to uphold fundamental EU rights and allows mass surveillance abuses by the U.S.[20] Although the hearing was originally scheduled for July 2019, it was suspended by the CJEU until the resolution of *Schrems II*.[21] The two cases will have major implications not only for trans-Atlantic data transfers, but also the world economy.

Privacy Shield Enforcement in the U.S.

The recent challenges to the adequacy of the Privacy Shield Framework come despite increased enforcement of the Privacy Shield principles by the DOC and FTC. After the European Parliament passed a resolution in July 2018 threatening to suspend the Privacy Shield,[22] the DOC and FTC have stepped up enforcement. The DOC updated its policies and committed to increased oversight, including random web searches for false claims of compliance and quarterly "false claims reviews" to identify organizations that have not completed certification or recertification.[23]

The FTC has also committed to make enforcement of the framework a high priority, announcing a sweep of Privacy Shield actions this year.[24] The FTC requires companies participating in the Privacy Shield framework to have an "independent recourse mechanism" to resolve individual disputes and procedures for verifying compliance.[25] Where an organization fails to comply with the sanctions rulings of independent recourse mechanisms, those

continued on page 6

Continued from 5

authorities are required to notify the FTC or the DOC.[26] The FTC may challenge the practices of participating U.S. companies under Section 5 of the Federal Trade Commission Act as "deceptive" and obtain court orders and even fines of up to $40,000 per violation.[27]

Given the recent commitment to robust enforcement of the Framework, it is critical that a business that has certified to compliance with the Privacy Shield Framework remain compliant with its requirements and closely monitor any changes to the Framework.

Looking Ahead

Given the unsettled international data transfer landscape, U.S. companies that rely on these mechanisms should keep a close eye on developments that could lead to new legal obligations. Transferring personal data to the U.S. without implementing a valid transfer mechanism can result in significant fines and penalties. In the event that the CJEU invalidates both or either of the contemporary mechanisms, companies should be prepared to revisit alternate pathways – including consent, derogations, or BCRs – to ensure GDPR-compliant data transfers. ■

For more information, please contact:

Joan Stewart
202.719.7438 | jstewart@wileyrein.com

———

[1] A survey by the International Association of Privacy Professionals found that among 370 privacy leaders polled, 88% used standard contractual clauses last year. As of October 5, there are 4,986 organizations registered under the Privacy Shield. *See* Department of Commerce, *Privacy Shield Framework*, https://www.privacyshield.gov/list (accessed Oct. 5, 2019); Catherine Stupp, *Companies Face Uncertainty Over Challenges to Trans-Atlantic Data Transfers*, The Wall Street Journal (Sep. 23, 2019, 11:18 AM), https://www.wsj.com/articles/companies-face-uncertainty-over-challenges-to-trans-atlantic-data-transfers-11569013484?mod=searchresults&page=1&pos=2&mg=prod/com-wsj.

[2] Jennifer Baker, *EU High Court hearings to determine the future of Privacy Shield, SCCs*, IAPP (June 25, 2019), https://iapp.org/news/a/eu-high-court-hearings-to-determine-future-of-privacy-shield-standard-contractual-clauses/.

[3] These include La Quadrature du Net, French Data Network and Fédération FDN.

[4] La Quadrature du Net, *Hearing Against the Privacy Shield Before the General Court of the EU* (May 24, 2019), https://www.laquadrature.net/en/2019/05/24/hearing-against-the-privacy-shield-before-the-general-court-of-the-eu/.

[5] Regulation 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) Article 44, 45, 46 (May 4, 2016) [hereinafter GDPR].

[6] *See* Resolution on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield, Eur. Parl. Doc. P8_TA-PROV(2018)0315 (2018), http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf.

[7] *See* Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

[8] Privacy Shield, *How to Join Privacy Shield*, https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 (accessed Oct. 6, 2019); Privacy Shield, *Requirements of Participation*, https://www.privacyshield.gov/article?id=Requirements-of-Participation (accessed Oct. 6, 2019).

[9] *See id.*

[10] Federal Trade Commission, *Privacy Shield,* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield (accessed Oct. 6, 2019).

[11] A survey by the International Association of Privacy Professionals found that among 370 privacy leaders polled, 88% used standard contractual clauses last year. Department of Commerce, *Privacy Shield Framework*, https://www.privacyshield.gov/list (accessed Oct. 5, 2019).

[12] European Commission, *Standard Contractual Clauses (SCC),* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed Oct. 5, 2019).

[13] *See* GDPR Article 46.

[14] Ashley Gorski, *EU Court of Justice Grapples with U.S. Surveillance in Schrems II,* Just Security (July 26, 2019), https://www.justsecurity.org/65069/eu-court-of-justice-grapples-with-u-s-surveillance-in-schrems-ii/.

[15] *Id.*

[16] Jennifer Baker, *CJEU's hearing on Schrems II has both sides worried ruling could be sweeping,* IAPP (July 9, 2019), https://iapp.org/news/a/cjeus-hearing-on-schrems-ii-has-both-sides-worried-ruling-could-be-sweeping/.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] La Quadrature du Net, *Hearing Against the Privacy Shield Before the General Court of the EU* (May 24, 2019), https://www.laquadrature.net/en/2019/05/24/hearing-against-the-privacy-shield-before-the-general-court-of-the-eu/.

[21] Baker *supra* note 30.

[22] *See generally* Privacy Shield Adequacy Resolution.

[23] *See* European Data Protection Board, *EU - U.S. Privacy Shield - Second Annual Joint Review* (Jan. 22, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf.

[24] *See* Federal Trade Commission, Privacy Shield, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield (*accessed* Oct. 7, 2019).

[25] Department of Commerce, *Enforcement of the Privacy Shield,* https://www.privacyshield.gov/article?id=Enforcement-of-Privacy-Shield (accessed Oct. 5, 2019).

[26] *Id.*

[27] *Id.*

FTC Pushing to Hold Companies Liable for Third Parties' Activities

By Duane C. Pozza

Recent Federal Trade Commission (FTC) enforcement actions and public statements have shown a renewed focus on trying to hold companies – including technology platforms and other companies dealing with consumer data – accountable for the activities of third parties. In a range of circumstances, the FTC has sought to place the onus on companies to police the conduct of companies that use their platform or with which they do business. This has particular relevance for companies that handle large amounts of consumer data and/or provide platforms that allow for user-generated content. The current Commission has already demonstrated its heightened expectations of companies' third-party monitoring obligations.

The FTC's recent **settlement** with YouTube clearly demonstrated its commitment to shift compliance obligations to platforms. That settlement requires the service to modify its technology platform to allow greater monitoring of third parties' COPPA compliance – beyond that required by law. The FTC's COPPA Rule requires certain online operators to obtain parental consent and take other steps if their services are directed to children under the age of 13. The FTC order requires the platform to implement a system for third parties to designate whether their service is directed to children – as the Chairman and Commissioner Wilson describe it in their **joint statement**, "the first and only mandated requirement on a platform or third party to seek actual knowledge of whether content is child-directed." That monitoring system is not required by COPPA, and indeed the Chairman's statement pointedly notes that "this relief will change YouTube's business model going forward." Moreover, Commissioner Slaughter dissented from the settlement on the theory that the order should have imposed *greater* burdens on the platform to monitor third parties for COPPA compliance.

In other circumstances, the FTC has suggested that it will look "up the chain" at platforms to determine if they should be held liable for misconduct by others. For example, testifying at a September 25 hearing before the U.S. House Subcommittee on Financial Services and General Government, Commissioner Chopra suggested that in investigating fraud, the Commission should look at payment facilitators and companies providing the infrastructure for wrongdoing. This kind of scrutiny could be based on an "unfairness" theory, which requires showing that the practice caused or was likely to cause substantial injury to consumers that could not be reasonably avoided, and that was not outweighed by countervailing benefits to consumers or competition. One recent example of this theory is a **complaint filing** against Match Group, which includes an allegation that the company "exposed" consumers to a risk of fraud from scammers on the company's dating website, which the Commission alleged to be unfair.

And outside of platforms, the FTC has scrutinized companies that obtain consumer data from third parties through allegedly unlawful means. In August, for example, the FTC settled a case with Career Education Corporation, an operator of for-profit schools, alleging that it was responsible for a significant number of unwanted telemarketing calls. Additionally, the FTC **alleged** that the company was responsible for deceiving consumers when its customer lead generators – who were vendors that it paid for customer referrals – allegedly made deceptive statements to consumers in the course of obtaining their information. The complaint alleged that it knew deceptive conduct was ongoing, but continued to accept consumer leads from the companies. In a recent **article**, the Director of the Bureau of Consumer Protection, Andrew Smith, stated his view that companies should adhere to higher standards when dealing with customer data they obtain from third parties – reasoning that could be extended outside this case-specific context. He highlighted due diligence obligations, contractual

continued on page 8

In Brief

The Proposed 'Honest Ads Act' Questioned on Privacy Grounds

Former FEC Chairs Lee Goodman, Michael Toner, and Professor of Law Bradley A. Smith have published an opinion editorial in *The Wall Street Journal* highlighting First Amendment privacy problems with the Honest Ads Act pending in Congress. The authors explain that the bill would invade the political privacy of American citizens who desire to speak about political subjects in paid ads online and impose serious burdens on the free press rights of online advertising platforms. The authors argue there are stronger mechanisms to address foreign meddling in U.S. elections that do not violate the free speech rights of American citizens.

The full article can be read **here**.

Lee Goodman can be reached at 202.719.7378 or **lgoodman@wileyrein.com**. Michael Toner can be reached at 202.719.7545 or **mtoner@wileyrein.com**.

FTC Pushing to Hold Companies Liable for Third Parties' Activities

Continued from 8

compliance standards, audit rights, monitoring, and even requirements that vendors monitor their subcontractors – "fourth parties" – for violations.

The current Commission continues to be aggressive on enforcement priorities, and the support for all of the legal theories above was unanimous. Companies should pay close attention to their interactions with third parties that may invite scrutiny from the FTC, and recognize that this Commission's expectations are increasing. ■

For more information, please contact:

Duane C. Pozza
202.719.4533 | dpozza@wileyrein.com

Speeches & Events

AI and Automation Regulation
Salt Lake City County Conference - The Future of Jobs
Duane C. Pozza, Speaker
October 16, 2019 | Salt Lake City, UT

ETA Spotlight Call: State Privacy Laws
Electronic Transactions Association (ETA)
Duane C. Pozza, Speaker, Antonio J. Reynolds, Speaker
October 23, 2019

Artificial Intelligence in Online Small Business Lending
Electronic Transactions Associations (ETA)
Duane C. Pozza, Speaker
October 25, 2019 | Washington, DC

U.S. Privacy Update: Developments at the Federal and State Level
Plumbing Manufacturers International 2019 Conference
Joan Stewart, Speaker
November 6, 2019 | St. Petersburg Beach, FL

California Consumer Privacy Act: Latest Developments and Compliance Strategies
Wiley Rein Webinars
Duane C. Pozza, Speaker, Antonio J. Reynolds, Speaker, Kathleen E. Scott, Speaker, Joan Stewart, Speaker
November 7, 2019

Robocall Regulatory Super-Session – Current Legislative and Regulatory Actions and Their Requirements and Ramifications.
The SIP Network Operators Conference "Focus on STIR/SHAKEN"
Kevin G. Rupy, Moderator
December 3, 2019 | Herndon, VA

Webinar and Podcast Library

September 12, 2019
Wiley Rein Partners Megan Brown and Katy Ross, and NTIA's Acting Administrator, Diane Rinaldo, discuss 5G, Huawei, and National Security
Wiley Rein National Security Webinar + Podcast Series
Megan L. Brown, Katy M. Ross

July 18, 2019
The Latest Regulatory Developments in AI
Wiley Connected
Duane C. Pozza, Jacquelynn Ruff

July 17, 2019
Latest Update on State Privacy and Security Laws: California and Beyond
Wiley Rein Webinars
Duane C. Pozza, Matthew J. Gardner, Joan Stewart, Kathleen E. Scott

March 26, 2019
Biometrics News
Wiley Rein Webinars
Duane C. Pozza, Kathleen E. Scott

March 20, 2019
Mobile World Congress: A Discussion on 5G and the Future of the Mobile Industry
Wiley Connected
Scott D. Delacourt, Jacquelynn Ruff

March 19, 2019
What to Watch: FTC Forecast for 2019
Wiley Rein Webinars
Megan L. Brown, Scott D. Delacourt, Duane C. Pozza

March 13, 2019
California Consumer Privacy Act (CCPA) Briefing
Wiley Rein Webinars
Matthew J. Gardner, Kathleen E. Scott, Joan Stewart

March 4, 2019
Federal Privacy Update: Congress, NIST & More
Wiley Rein Webinars
Megan L. Brown, Duane C. Pozza, Kathleen E. Scott

January 7, 2019
Blockchain, Trust, and Regulation: A Conversation with Wharton Professor Kevin Werbach
Wiley Connected
Duane C. Pozza

November 30, 2018
Advanced Persistent Chats: DHS's Cybersecurity and Infrastructure Security Agency Podcast
Wiley Connected
Megan L. Brown, Michael L. Diakiwski

October 30, 2018
Podcast: How Much Do You Know About Blockchain Policy? An Interview with the Blockchain Association's Director of External Affairs, Kristin Smith
Wiley Connected
Matthew J. Gardner

Privacy and Cybersecurity at Wiley Rein

Rachel A. Alexander	202.719.7371	ralexander@wileyrein.com
Daniel P. Brooks	202.719.4183	dbrooks@wileyrein.com
Megan L. Brown	202.719. 7579	mbrown@wileyrein.com
Moshe B. Broder	202.719.4186	mbroder@wileyrein.com
Jon W. Burd	202.719.7172	jburd@wileyrein.com
Scott D. Delacourt	202.719.7549	sdelacourt@wileyrein.com
Michael L. Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Boyd Garriott	202.719.4487	bgarriott@wileyrein.com
Lee E. Goodman	202.719.7378	lgoodman@wileyrein.com
Peter S. Hyun*	202.719.4499	phyun@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Dorthula H. Powell-Woodson	202.719.7150	dpowell-woodson@wileyrein.com
Duane C. Pozza	202.719.4533	dpozza@wileyrein.com
Antonio J. Reynolds	202.719.4603	areynolds@wileyrein.com
Jacquelynn Ruff	202.719.7224	jruff@wileyrein.com
Kevin G. Rupy	202.719.4510	krupy@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com
Joan Stewart	202.719.7438	jstewart@wileyrein.com

*Not admitted to the District of Columbia Bar. Supervised by principals of the firm who are members of the District of Columbia Bar.

To update your contact information or to cancel your subscription to this newsletter, visit:

www.wileyrein.com/newsroom-signup.html.