Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | November 2019

We begin this issue with a deep dive into the draft Attorney General regulations to implement the California Consumer Privacy Act (CCPA). We distill 10 key points to know about the draft regulations, in an article by myself, Joan Stewart, and Kat Scott. And there are many more details about the CCPA that will affect compliance – for more resources you can view our **webinar** or contact us directly. Our privacy team will also be hosting an **event** on Wednesday, December 4, in San Francisco that will include our takeaways from the AG hearings that week.

The CCPA is hardly the only issue to watch. In this issue, Lee Goodman analyzes two recent court decisions restraining enforcement of political disclosure laws. I discuss recent remarks by two FTC Commissioners on how the FTC's approach to privacy policy and enforcement will continue to evolve. And Megan Brown and Boyd Garriott examine a split in the Courts of Appeals over standing requirement for bringing privacy cases (and specifically under the Illinois Biometric Information Privacy Act) – which may be headed to the U.S. Supreme Court.

Feel free to reach out to anyone on our privacy team, as always. I can be reached at 202.719.4533 or **dpozza@wileyrein.com**. We will be on hiatus in December, but back in January. Happy holidays!

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

Ten Things You Need to Know About the CCPA Draft Regulations

By Duane E. Pozza, Joan Stewart, and Kathleen E. Scott

On October 10, 2019, the California Attorney General released draft regulations to implement the California Consumer Privacy Act (CCPA). While the draft regulations clarify some obligations under the statute, they also potentially add to a business's compliance burden and create uncertainty in several areas. The regulations are not final and are open for comment until December 6, meaning that in all likelihood, we will not see the final regulations until well after the CCPA goes into effect on January 1, 2020.

Amid this uncertainty, we are helping clients manage compliance strategies for the CCPA, including the new compliance obligations proposed in the draft regulations. Informed by the draft regulations, here are 10 key points to consider when planning for CCPA compliance:

continued on page 2

IN THIS ISSUE:

Continued from 1

1. Your Privacy Policy Will Need Significant Updates.

The statute and the draft regulations require a business to disclose very specific information in its privacy policy. This includes details about how personal information is collected; how personal information is sold or disclosed for a business purpose; what rights consumers have; how consumers may submit a request to exercise those rights; how a consumer may designate an authorized agent to submit requests; when the privacy policy was last updated; and how to contact the business. On top of this, some businesses that deal with a high volume of personal information, under the draft rules, would need to disclose specific metrics (discussed in more detail below).

At the same time, the privacy policy must be designed and presented to the consumer in a way that is "easy to read and understandable to an average consumer" – a difficult task given the volume of information that must be disclosed. It must also be accessible to consumers with disabilities. The statute and regulations do not specify how exactly this latter requirement should be met, so companies will need to look closely at standards and best practices.

2. The Draft Regulations Contemplate Multiple Consumer Notices.

The draft regulations contemplate three separate notices, in addition to the privacy policy: a notice at the time of collection of personal information, a notice of the right to opt out of the sale of information, and a notice of financial incentives (or price or service difference) for collection. While the draft regulations would allow these notices to either be stand-alone documents or included as separate sections within the privacy policy, each would need to have a separate, conspicuous link. The draft rules call for these links (in all cases but the link to the notice of financial incentive) to be found on a website's "homepage." Unfortunately, the draft regulations do not clear up the ambiguity created by the statute as to what constitutes a website "homepage." Additionally, the draft regulations explicitly exempt businesses that do not "sell" personal information from posting a notice of right to opt out, but *include* a requirement that the business affirmatively state that it "will not" sell personal information in the future – an obligation not found in the statute.

3. Offering Compliant Financial Incentives and Pricing Differences Is Complicated.

The draft regulations expand on (but complicate) the statute's guidance on how to offer compliant financial incentives and pricing differences. The CCPA prohibits discrimination against consumers based on the exercise of their CCPA rights, but permits financial incentives and price and service differences in limited circumstances. The CCPA requires that the price or service difference must be reasonably related to the value of the consumer's data. The draft regulations require a business to provide a detailed analysis of how the value is calculated and include an expansive list of factors to consider when estimating value, including the marginal or average value of the data to the business, revenue or profit generated by use of the data, or expenses related to collection or use of the data. Confusingly, the draft regulations define a "price or service difference" to include differences obtained through use of financial payments (that is, a "financial incentive"), and the notice and data valuation provisions suggest that businesses must also calculate data valuation for both financial incentives and price or service differences (though this requirement is not in the CCPA itself). Bottom line: Businesses will need to carefully think through any differential treatment of consumers based on collection, sale, or ability to delete their data.

4. The Process to Verify a Consumer Request Is Elaborate, but Not Well-Defined.

Under the draft regulations, a business needs to establish a "reasonable method" for verifying the identity of an individual who submits a request to

continued on page 3

Continued from 2

know or a request to delete (though notably, not a request to opt out of sale). A business should, where feasible, match the identifying information provided by the consumer to personal information the business already maintains, or use a third-party verification service to do the same, but should avoid collecting new information or certain sensitive information (such as a Social Security Number) unless "necessary" for verification. The regulations also require that the verification process be tailored to the type of information requested and the risk of harm posed by unauthorized access or deletion of that information. In short, the regulations will require a careful balancing act of being responsive to a consumer request and protecting information from disclosure to unauthorized third parties.

5. A Consumer's Right to Know May Require a Personalized and Detailed Response.

The draft regulations provide detailed requirements for responding to requests to know, which in some cases goes beyond the statute. First, consider timing – per the statute, there is a 12-month "look back" on consumers' data, meaning that consumers can request information about the collection, use, disclosure, and sale of their personal information for the 12-month period prior to the request. Since the law takes effect January 1, 2020, that means businesses must be prepared to receive requests about personal information during all of 2019 (when the law was not in effect). Consumers have the ability under the statute and draft regulations to request detailed information that a business has collected about them. The CCPA contemplates that the response to the consumer would be customized, not a generic response. The consumer could ask for the categories of information that the business has collected about them or could request specific pieces of data collected about them during the past year. A business must be ready to respond to each type of request, and there are different requirements for doing so. For example, there are various security considerations and requirements around transmitting specific pieces of data. Additionally, the business must be prepared to disclose the purpose of the collection, categories of third parties to whom information was disclosed, and the business or commercial purpose for the disclosure.

6. Responding to a Request for Deletion – Pay Attention to the Deadlines.

The draft regulations propose to require a business to confirm receipt of a consumer's request within 10 days and comply with the request within 45 days. These same deadlines apply to a request to know. The business can extend its deadline by an additional 45 days if it notifies the consumer. If the business denies the request for deletion, it must explain why. Depending on its reason for denying the request, a business may create additional obligations for itself. For example, if the denial is based on inability to verify the identity of the consumer, it must nevertheless treat it as a request to opt out of sale (which does not require verification).

7. The Regulations Impose Specific Obligations for the Right to Opt Out.

The CCPA's right to opt out is perhaps its best-known consumer right. The draft regulations provide additional context, but also additional requirements for a business that sells information. The draft regulations confirm that a business must have a prominent hyperlink on its website declaring "Do Not Sell My Information" or "Do Not Sell My Info." The draft regulations contemplate that a consumer could use an authorized agent to exercise their rights, including the right to opt out. However, the regulations also encourage a business to verify that an authorized agent is acting on at the individual's request. The draft regulations require a shorter response time for requests to opt out than that proposed for the other rights. A business is required to act on a request to opt out "as soon as feasible possible" but no later than 15 days. Additionally, it must pass that request down the chain of third parties to which it has sold the consumer's information within the preceding 90 days.

continued on page 4

Continued from 3

8. If Your Business Collects Information About Consumers Indirectly, It Has Obligations.

Some businesses may obtain personal information indirectly – either as "service providers" or because a business purchases or otherwise obtains personal information from another business. If the business is acting as a service provider, ensure there is a written contract in place with the required CCPA language that prohibits the business from using or disclosing the information for any purpose other than the contractual business purpose. If the business has otherwise obtained personal information about a consumer indirectly, then the draft regulations require that before **selling** that information, the business must contact the consumer directly to provide an opt-out notice (or, alternatively, contact the source from which your business received the personal information and obtain a signed attestation that the consumer received a notice at collection).

9. For a Business That Deals with a High Volume of Personal Information, the Draft Regulations Propose Heightened Disclosure Requirements.

The draft regulations introduce wholesale new requirements for businesses that buy, receive, sell, or share for commercial purposes the personal information of 4 million or more consumers. These businesses would be required to provide very detailed disclosures in their privacy policies or on their websites of: (1) the number of requests to know/delete/opt out (including the number approved and denied), and (2) the median number of days it took the business to respond to those requests. Additionally, these businesses must implement a training program for their employees who handle consumer requests (which is a requirement under the CCPA for all businesses).

10. Don't Forget the "Other" California Privacy Rules.

The CCPA and draft regulations notably do not reference the existing California laws that govern privacy policies and practices, including the California Online Privacy Protection Act (CalOPPA) and California's Shine the Light law. CalOPPA, for example, requires commercial websites and online services to post a privacy policy and requires disclosures regarding tracking of online visits. As you are updating your policies and practices to be compliant with the CCPA, it is important not to overlook these other laws. ■

For more information, please contact:

Duane C. Pozza
202.719.4533 | dpozza@wileyrein.com

Joan Stewart
202.719.7438 | jstewart@wileyrein.com

Kathleen E. Scott
202.719.7577 | kscott@wileyrein.com

Courts Reject Overbroad Compulsory NJ/NY Disclosure Laws

By Lee E. Goodman

Two federal courts recently have restrained enforcement of overbroad compulsory donor disclosure and related disclosure laws on the basis of First Amendment privacy concerns. Considered together, these court rulings reaffirm First Amendment protection for political privacy and anonymity in political speech and association. They also signal caution to legislators and regulators that the courts will impose meaningful constitutional boundaries around government efforts to compel public registration and disclosure of political activities.

Citizens Union v. New York

In 2016, the New York legislature passed, and Governor Cuomo signed, a new ethics law that required each nonprofit 501(c)(3) organization to disclose its contributors of $2,500 or more whenever the organization contributed $2,500 in a six-month period to a social welfare 501(c)(4) organization. It also required 501(c)(4) groups that spend over $10,000 a year on issue advocacy to disclose their contributors of $1,000 or more. The law was challenged in the U.S. District Court for the Southern District of New York as a violation of the First Amendment by nonprofit organization Citizens Union of the City of New York and other nonprofit groups.

"There is no question," the court started its analysis, "that public disclosure of donor identities burdens the First Amendment rights to free speech and free association." The court surveyed historical precedents – including the often discounted U.S. Supreme Court opinions in *McIntyre v. Ohio* (1995), *Talley v. California* (1960), and *NAACP v. Alabama* (1958), as well as the Supreme Court's seminal decision in *Buckley v. Valeo* (1976) – and divined a clear line between election advocacy, which can be regulated through compelled donor disclosure, and issue advocacy, which generally cannot be so regulated.

The court, applying a muscular version of the "exacting scrutiny" standard, then assessed whether there was any "substantial relation" between public identification of donors and New York's asserted interests in providing citizens information, deterring corruption, and detecting violations of the law. The court found that the compelled
disclosure of 501(c)(3) donors was not justified in light of the "tangential and indirect support of political advocacy" covered by the law. Among other weaknesses, the court found the relationship between a 501(c)(3)'s donors and electioneering or direct lobbying "too attenuated to effectively advance any informational interest." Many donors contribute to a nonprofit's general treasury without earmarking their contributions to a subsequent donee 501(c)(4) organization.

The court also struck the law's requirement for 501(c)(4) groups to disclose their donors if they engage in issue advocacy. The court first considered the breadth of the topics covered by disclosure, which included any elected official's "position" on legislation or potential legislation. The court observed that "any matter of public importance could become the subject of legislation and given the range of positions taken by all elected officials," which the court termed "pure issue advocacy." Indeed, the "government acknowledges that the government interest at stake is the interest in revealing 'the funders of issue advocacy,'" the court rereported. "The cases upholding donor disclosure requirements have never recognized an informational interest of such breadth." The court also distinguished the breadth of the issue advocacy covered by the New York law and the narrow "electioneering communication" definition at issue in and upheld by the Supreme Court in *McConnell v. FEC* (2003). Accordingly, the court struck the compulsory disclosure laws for both 501(c)(3) and 501(c)(4) organizations as violative of the First Amendment.

Americans for Prosperity v. New Jersey

In 2019, the New Jersey legislature passed, and Governor Murphy signed (subject to expressed constitu-

continued on page 6

Courts Reject Overbroad Compulsory NJ/NY Disclosure Laws

Continued from 5

tional reservations), S1500, which required 501(c)(4) and 527 organizations that spend as little as $3,000 in a calendar year on "influencing or attempting to influence the outcome" of any election, public question, legislation or regulation, or that merely "provide any political information" about any candidate, public question, legislation or regulation, to file quarterly reports publicly disclosing the names of all contributors who donated $10,000 or more. The law's coverage included activities such as voter registration, polling, research, and get-out-the-vote drives, even if they were nonpartisan. The law was challenged facially and as-applied under the First Amendment by nonprofit 501(c)(4) organization Americans for Prosperity, which moved first for a preliminary injunction.

Like its sister court in New York, the federal court in New Jersey started by acknowledging that "compelled identification of contributors to independent groups that expend money on political causes 'can seriously infringe' the rights to privacy of association and to belief guaranteed by the First Amendment." The court cited *Buckley v. Valeo* and *NAACP v. Alabama*. The court also relied upon the critical distinction *Buckley* drew between issue advocacy and election advocacy. The New Jersey court quoted the *Buckley* formulation for exacting scrutiny to require that a law "furthers a vital governmental interest … that is achieved by a means which does not unfairly or unnecessarily burden either a minority party's or individual candidate's equally important interest in the continued availability of political opportunity." Finally, the court held the government responsible for undesirable public attention visited by compelled disclosure.

The court concluded there was no "substantial relation between the disclosure requirement and a sufficiently important governmental interest" because it was patently overbroad. The court cited three main reasons. First, the law required disclosure of donors for merely "political information," even "purely factual information" about public officials and their votes in office, such as a "scorecard" informing citizens how a public official voted. Second, it applied to communications over virtually all possible media. Third, it applied to activities from January 1 through election day in November.

Accordingly, the court issued a preliminary injunction prohibiting the state from enforcing the compulsory disclosure law based on the likelihood that it facially violated the First Amendment. The court reserved judgment on the plaintiff's as-applied challenge, although it expressed sympathy for the claim, noting what it called the current "climate marked by the so-called cancel or call-out culture that has resulted in people losing employment, being ejected or driven out of restaurants while eating their meals; and where the Internet removes any geographic barriers to cyber harassment of others."

Conclusion

The Supreme Court's seminal decision in *Buckley v. Valeo* (1976) figured centrally in each decision. Specifically, the courts observed the critical line *Buckley* drew between *election* advocacy versus *issue* advocacy. Another common thread was application of a muscular "exacting scrutiny" standard of review that came closer to "strict scrutiny" than the "rational basis" review that other courts recently have applied. Applying these principles, the federal courts in New York and New Jersey found facial infirmities with the state laws. The New York and New Jersey rulings are likely to be appealed to the Second and Third Circuits, respectively, which have tended to be more deferential to government compelled disclosure requirements.■

For more information, please contact:

Lee E. Goodman
202.719.7378 | lgoodman@wileyrein.com

FTC Commissioners Give Key Insights on Privacy Views

By Duane C. Pozza

In remarks on Monday, October 28 at the Brookings Institution, FTC Commissioners Rebecca Slaughter and Christine Wilson spoke extensively about the Commission's privacy outlook and their personal views on the national privacy debate. While from different parties, they were largely in agreement on a number of key points – reflecting how the current Commission has continued to move towards more aggressive enforcement on privacy and data governance. The willingness of these Commissioners to be so direct on a wide range of topics helps point to where the Commission is headed on future enforcement, and in making recommendations to follow up on its **Hearings on Competition and Consumer Protection in the 21st Century**. Some key questions and answers are summarized here:

Should our privacy laws focus primarily on "notice and choice" – giving consumers the opportunity to understand how data is collected and used, typically through privacy policies? The Commissioners' answers were basically "no". Commissioner Slaughter said she was "over" a notice and consent framework, arguing that neither the notice or choice was meaningful for consumers. Commissioner Wilson emphasized that her views have evolved over time, suggested that notice and choice has a limited role to play, and argued that clear and transparent rules about data use would benefit both business and consumers. The FTC has long brought cases under its deception authority – policing the "notice" portion of "notice and choice" by arguing that companies violated their privacy representations to consumers – but it seems the Commission is increasingly looking to examine a broader set of practices.

Will the FTC focus only on specific, demonstrable injuries that flow from privacy violations? Again, the answer appears to be "no". In the context of private rights of action, the need to show demonstrable injury is an **issue** that could soon reach the Supreme Court. In her remarks, Commissioner Wilson largely stuck to existing cases the FTC has brought, which have used an elevated risk of harm (including non-financial harm) to justify action. Commissioner Slaughter was clear that the Commission should not need to allege a specific concrete harm based on unwanted disclosure of private information – pointing for example to identity theft, where the use of stolen data for harm can be delayed and difficult to track down.

Are there other harms from data use the FTC should address? Commissioner Slaughter identified targeted advertising based on collected information as a potential "harm" to be addressed in certain circumstances. And overall, she framed the "privacy" discussion as a broader one about what she termed "data abuses," focusing on harmful uses of data. When asked about whether algorithmic biases should be concerning, Commissioner Wilson pointed to the Commission's 2016 **Big Data** report, which outlines ways in which algorithmic biases could give rise to concerns under existing laws like the Fair Credit Reporting Act or Equal Credit Opportunity Act. Commissioner Slaughter went further, referring to certain kinds of bias from algorithmic decision making as a "data abuse" that warranted action.

Should there be monetary penalties in privacy cases? The Commission now **supports** Congress granting civil penalties for first-time privacy violations. And the Commission supports closing the common carrier and non-profit exemptions, meaning that a greater swath of companies (for example, non-profit hospitals) would be subject to the FTC's privacy enforcement.

As much of the FTC's work and its deliberations are confidential, it can sometimes be difficult to tell what policy and enforcement actions are being considered. But these and other recent remarks by Commissioners point strongly toward a heightened emphasis on enforcement in the areas of privacy and companies' data practices more generally. ■

For more information, please contact:

Duane C. Pozza
202.719.4533 | dpozza@wileyrein.com

How Patel v. Facebook Might Tee Up a Privacy Battle at the Supreme Court

By Megan L. Brown and Boyd Garriott

In August, the Ninth Circuit issued an important decision on privacy and Article III standing in **Patel v. Facebook**. And while the decision is sure to have far-reaching consequences, it may trigger a fight at a court with even farther-reaching consequences: the Supreme Court. This is because Patel appears to create a circuit split with a Second Circuit decision from 2017, **Santana v. Take-Two Interactive Software, Inc.**

Both cases deal with a state privacy law called the Illinois Biometric Information Privacy Act (BIPA). BIPA imposes numerous procedural obligations on organizations that collect biometric information, such as fingerprints. To name a few, it requires obtaining written consent before collecting biometric information and publishing a data retention schedule. BIPA also provides a private right of action to any person "aggrieved" by violations of the Act. In January, the Illinois Supreme Court **held** that merely violating the procedural provisions of BIPA — without any showing of actual harm—was sufficient to bring a suit seeking liquidated damages in state court. (Our summary of that decision is available **here**). The question in *Patel* and *Santana* was whether the same was true in federal courts, given the higher bar of Article III standing.

In *Patel*, plaintiffs alleged that the defendant violated the procedural provisions of BIPA by not taking actions like publishing a retention schedule about how long it would keep data that it collected using facial recognition software. However, the plaintiffs did not allege any substantive harm. That is, no one accused the defendant of mishandling or inadvertently releasing any information. The defendant moved to dismiss on Article III standing grounds. However, the Ninth Circuit held that merely failing to comply with BIPA's procedural provisions is a sufficient harm for plaintiffs to satisfy Article III standing. (For more information, our full summary of *Patel v. Facebook* is available **here**).

The Ninth Circuit's decision in *Patel* contrasts starkly with the Second Circuit's 2017 summary order in *Santana*. In *Santana*, the Second Circuit examined a basketball video game that scanned individuals' faces to create custom in-game avatars. The plaintiffs sued, alleging, among other things, that the video game publisher "did not inform them of the duration that it would hold their biometric data, as BIPA requires." The Second Circuit found that the plaintiffs lacked standing for this claim because they did not allege that this deficient notice created any material risk that would have "resulted in plaintiffs' biometric data being used or disclosed without their consent."

The conflict is straightforward. *Patel* held that mere procedural violations of BIPA — without more — are *sufficient* for Article III standing, but *Santana* held that violations of the exact same BIPA procedures — without more — are *insufficient* to confer Article III standing. There are also several district court opinions that appear to conflict with *Patel*. *See e.g., Rivera v. Google, Inc.*, 366 F. Supp. 3d 998, 1014 (N.D. Ill. 2018) (dismissing case alleging BIPA violations for facial recognition scans because "Plaintiffs have not demonstrated an injury-in-fact sufficient to confer Article III standing"); *McGinnis v. United States Cold Storage, Inc.*, 382 F. Supp. 3d 813, 820 (N.D. Ill. 2019) (dismissing case alleging BIPA violations for requiring employees to scan fingerprints because plaintiff did not "allege[] a concrete injury sufficient to satisfy Article III").

There are two wrinkles to this analysis, but neither affects the underlying split. *First*, *Santana* is a summary order, which does not create binding precedent in the Second Circuit. However, the Supreme Court has **previously** granted cert to resolve a split where one circuit's opinion was "an unpublished order." *Second*, the **district court opinion** in *Patel* tried to distinguish *Santana* on the ground that the plaintiffs in *Santana* were aware that

continued on page 9

How Patel v. Facebook Might Tee Up a Privacy Battle at the Supreme Court

Continued from 8

their biometric data was being collected, allegedly unlike the plaintiffs in *Patel*. However, that ultimately appears to be a distinction without a difference, as the district court (and the Ninth Circuit) found that "the abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury." In other words, if procedural violations of BIPA are all that is required to allege a concrete injury, then the question of notice is irrelevant under those courts' logic.

So why does this circuit split matter? The **Supreme Court's rules** enumerate a list of (non-exhaustive) reasons for what the Justices consider in determining whether to grant certiorari. One of these reasons is whether "a United States court of appeals has entered a decision in conflict with the decision of another United States court of appeals on the same important matter . . ." Since **Spokeo v. Robins**, the Supreme Court has been **extremely reluctant** to take up any privacy-related standing cases, despite the fact that the lower courts have begun to diverge—as evidenced by *Patel*. The split caused by the Ninth Circuit's *Patel* decision may change this.

Indeed, the defendant in *Patel v. Facebook* has already indicated that it will file for certiorari. On October 24, the defendant filed a motion to stay the issuance of the court's mandate pending a cert petition. The Ninth Circuit granted that motion on October 30. Interested parties should keep an eye out for the cert petition anytime between now and mid-January.■

For more information, please contact:

Megan L. Brown
202.719.7579 | mbrown@wileyrein.com

Boyd Garriott
202.719.4487 | bgarriott@wileyrein.com

In Brief

Duane Pozza Testifies Before U.S. House Financial Services Committee's Fintech Task Force

Duane C. Pozza, partner in Wiley Rein's **Telecom, Media & Technology (TMT)** and **Privacy, Cyber & Data Governance** practices, testified on November 21, 2019 before the U.S. House Financial Services Committee's Task Force on Financial Technology (Fintech). The **hearing**, titled "Banking on Your Data: The Role of Big Data in Financial Services," addressed the increased use of big data in financial services, which has led to the rapid development of new products and services.

In his **written testimony** to the task force, Mr. Pozza discussed the enormous potential for data-driven financial services to improve consumers' financial lives, as well as the regulatory landscape and how new privacy laws affect fintech.

"Companies can use consumer data responsibly to expand access to credit, provide customized financial advice, detect and prevent fraudulent behavior, and provide financial services at a lower cost," Mr. Pozza said. "Companies are already using large and robust data sets to accomplish these objectives, and the development of machine learning and artificial intelligence (AI) technologies will further advance what technology innovators can accomplish," he added.

Also testifying at today's hearing were Lauren Saunders, associate director of the National Consumer Law Center; Seny Kamara, associate professor of Computer Science at Brown University and chief scientist at Aroki Systems; Christopher Gilliard, professor of English at Macomb Community College and Digital Pedagogy Lab Advisor; and Don Cardinal, managing director at the Financial Data Exchange (FDX).

Rep. Maxine Waters (D-CA), Chairwoman of the House Committee on Financial Services, **announced** on May 19 the creation of the Task Force on Fintech, which examines U.S. and international fintech regulation, how fintech is used in lending, and how consumers engage with fintech.

Mr. Pozza previously served as Assistant Director in the Division of Financial Practices at the Federal Trade Commission's (FTC) Bureau of Consumer Protection. In that role, he helped organize the FTC's Fintech Forum Series, which examined a range of fintech innovation. He is a leading lawyer with respect to technological innovation, consumer protection, and enforcement, advising clients on key legal issues, advocacy positions, and regulatory compliance in such areas as privacy and security, the Internet of Things (IoT), AI and data analytics, mobile payments, and fintech lending.

To read Mr. Pozza's written testimony, please click **here**. A video of the hearing is available **here**.

Speeches & Events

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

State Privacy and Security Law Developments and Upcoming Challenges
American Tort Reform Association
Megan L. Brown, Speaker
November 12, 2019 | West Palm Beach, FL

The California Consumer Privacy Act (CCPA): Policy and Operational Issues, as January 1, 2020 Approaches
Federal Communications Bar Association
Duane C. Pozza, Speaker
November 19, 2019 | Washington, DC

U.S. Government Approach to 5G Innovation and Security
U.S. Chamber of Commerce
Megan L. Brown, Speaker
November 20, 2019 | Flowood, MS

AI Is Here: The Current State of AI Technology, Evolving Issues, and Policy Frameworks
Federal Communications Bar Association
Duane C. Pozza, Moderator
November 21, 2019 | Washington, DC

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

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

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 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

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.