Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | September 2018

Our articles this month focus on two hot topics. I look at the latest developments from the new California privacy law, which remains confusing and will have significant implications for a broad range of companies across the country. Megan Brown, Michael Diakiwski, and Kathleen Scott review the FTC's series of hearings related to its ongoing enforcement agenda for the future, related both to competition and consumer protection.

As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

An (Interim) Update on California's Privacy Law

By Kirk J. Nahra

You all know that California passed a massive privacy law in in June 2018. You may know how rapidly the bill (AB 375) was passed. And you probably also know that there's an enormous amount of confusion about what the California Consumer Privacy Act of 2018 (CCPA) will eventually say and what some of the key provisions mean. We have some interim news – but there's still a long way to go.

The Law Itself

Unlike most current U.S. national laws, the CCPA is intended to have general applicability, independent of industry sector. Essentially, a business that collects personal information about California residents is covered by this law, unless there is a defined exception. The big exceptions are (1) certain companies covered by other privacy laws (such as HIPAA and Gramm-Leach-Bliley) and (2) those with $25 million or less in annual revenue or which have personal information on fewer than 50,000 people or derive less than 50% of their revenue from sale of personal information.

There are major open issues even about this coverage. The law did not make clear whether the revenue threshold was for California or more generally. The status of nonprofits may

continued on page 5

FTC Hearings on Competition and Consumer Protection in the 21st Century

By Megan L. Brown, Michael L. Diakiwski and Kathleen E. Scott

The Federal Trade Commission (FTC or Commission) has begun a series of hearings on Competition and Consumer Protection in the 21st Century. As Wiley Rein noted previously, this is a major initiative that will help shape the agency's – and the entire federal government's – approach on issues critical to the digital economy. More specifically, the wide-ranging hearings will be of interest to a multitude of companies across industries – touching everything from global privacy and data security, to legal and regulatory frameworks, big data, and emerging technologies and their uses.

FTC Chairman Joe Simons described the hearings as intended to facilitate "serious reflection and evaluation" so that the Commission will be "better able to promote competition and innovation, protect consumers, and shape the law, so that free markets continue to thrive."

Preliminary Comments & Stakeholder Feedback

In advance of the hearings, the Commission **sought comments** in order to "examine whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy."

Hundreds of comments were filed across 11 topics selected by the Commission. Commenters included Fortune 100 companies, business associations, privacy advocates, academic institutions, state attorneys general, and members of Congress. Several of the Commission's selected topics relate to privacy and data security issues, including but not limited to:

- **Topic 2:** Competition and consumer protection issues in communication, information, and media technology networks
- **Topic 4:** The intersection between privacy, big data, and competition
- **Topic 5:** The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters
- **Topic 9:** The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics

A variety of commenters called for tighter rules and regulations related to privacy and data security. Several consumer advocacy groups argued that the Commission should formally ask Congress for greater authority related to rulemaking and levying penalties for privacy and data security violations. Others argued that informational harm, on which the FTC has held **workshops**, should not need to be proven by showing "substantial injury."

Members of Congress weighed in on the side of greater regulation of privacy and data security. **Rep. James Langevin** encouraged the Commission to pursue new tools to better deter negligent handling of personal or sensitive data. He proposed that the FTC's current remedial authority, under Section 5 of the FTC Act, may not adequately deter unfair and deceptive conduct in privacy and data

continued on page 3

continued from page 2

security matters. **Sen. Richard Blumenthal** argued that "[i]n light of recent technological advances, we need a stricter legal and regulatory framework to protect consumer privacy."

A group of **state Attorneys General**[1] emphasized the need to continue enforcing consumer protection laws related to privacy and data security. They contend that "consumer privacy and data security is an afterthought in product and service development. Industry often does not adequately invest in privacy and security. Consumer data has inherent value and the free market alone does not adequately protect sensitive data."

Industry feedback, however, pushed back on many of these notions. **AT&T** noted that "the Commission has properly relied on industry and multi-stakeholder processes rather than one-size-fits-all, top-down government regulation," and the Commission has "long supported a measured approach that protects consumers from genuine privacy abuses[.]" Further, AT&T wrote, "self-regulatory mechanisms are often superior to governmental mandates because, unlike prescriptive rules, multistakeholder processes provide the flexibility and speed necessary to address rapid technology and market changes." **BSA – The Software Alliance**, pointed to the benefits of emerging technologies, highlighting that artificial intelligence and machine learning are "revolutionizing how companies monitor network security," improving fraud detection and data security overall.

Some commenters praised the current U.S. approach to privacy, arguing that it is effective and does not need an overhaul. The **Association of National Advertisers** (ANA), for example, argued that "[t]he well-functioning U.S. privacy framework is composed of: (1) a federal regulatory scheme that is primarily sectoral and targeted; and (2) self-regulatory codes of conduct that effectively promote the responsible online and offline collection and use of data." ANA, in promoting the U.S. approach to privacy, argued that alternative approaches, like the California Consumer Privacy Act of 2018, will have adverse impacts on both competition and consumer protection. Similarly, the **Consumer Technology Association** (CTA) noted that, "the FTC should continue to promote a flexible and technology-neutral framework for privacy and security." Underscoring that "emerging fragmentation and inconsistent domestic and international regulatory approaches to privacy and security pose new challenges for companies and threaten to confuse consumers," CTA argued that the Commission "should continue to encourage industry to collaborate in global standardization efforts to develop technological best practices and standards, and also promote regulatory harmonization to increase economics of scales."

Many commenters emphasized that the Commission should support the harmonization of fragmented state, federal, and global privacy and data security regimes. **BSA** noted that "alone or with other agencies, and, crucially, in partnership with the industry

continued on page 4

[1] The Attorneys General from Arizona, Arkansas, California, Connecticut, Delaware, the District of Columbia, Florida, Hawaii, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Nebraska, New Jersey, New Mexico, New York, North Carolina, Oregon, Pennsylvania, Rhode Island, Tennessee, Vermont, Virginia, and Washington joined this filing.

continued from page 3

stakeholders who are on the front lines of our defense against sophisticated cyber threats," the FTC should consider ways in which it can help simplify the patchwork of complex and sometimes conflicting data security laws, rules, and standards. **ACT – The App Association** argued that policymakers should pursue a single, national standard for data security and that such a standard should incentivize innovation and allow for broad flexibility.

Other commenters also stressed the need for a balanced approach, aligning with the stated intention of Chairman Simons. The **Computer and Communications Industry Association** pointed to studies based on investments made in the tech sector in the European Union, arguing that "[p]rivacy laws and regulations can have an unintentionally adverse impact if they do not strike the correct balance between privacy and furthering innovation. Restricting companies' use and collection of data may unintentionally impair commerce in the digital economy, and by implication, reduce investment."

Hearing Schedule

On August 24, 2018, the FTC announced its opening round of hearings. The current schedule is as follows:

- **Hearing #1** – September 13-14: Review of Competition and Consumer Protection Landscape; Concentration and Competitiveness in U.S. Economy; Privacy Regulation; Consumer Welfare Standard in Antitrust; Vertical Mergers.
- **Hearing #2** – September 21: State of U.S. Antitrust Law; Mergers and Monopsony or Buyer Power.
- **Hearing #3** – October 15-17: The Identification and Analysis of Collusive, Exclusionary, and Predatory Conduct by Digital and Technology-Based Platform Businesses; Antitrust Framework for Evaluating Acquisitions of Potential or Nascent Competitors in Digital Marketplaces; Antitrust Evaluation of Labor Markets.
- **Hearing #4** – October 23-24: Innovation and Intellectual Property Policy.
- **Hearing #5** – November 6-7: Privacy, Big Data, and Competition.
- **Hearing #6** – November 13-14: Algorithms, Artificial Intelligence, and Predictive Analytics.

Looking Ahead

Currently, the FTC is seeking further comments on Hearing #1; these comments are due October 14, 2018.

On September 17, Wiley Rein is hosting a **roundtable discussion** with FTC Commissioner Maureen Ohlhausen. And on September 27, as part of the *Outlook on Cyber* speaker series, Wiley Rein is hosting Bilal Sayyed, Director of the FTC's Office of Policy Planning, and James Cooper, Deputy Director for Economic Analysis in the FTC's Bureau of Consumer Protection, for a discussion on the Commission's recent privacy and data security initiatives, including the ongoing hearings. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Michael L. Diakiwski
202.719.4081
mdiakiwski@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

be unclear. There is ongoing debate about whether employee information is covered, and many of the exceptions (such as whether the HIPAA exception applied to "business associates") were not at all clear. There is significant confusion about what "financial incentives" are permitted, and what financial considerations would constitute unpermitted discrimination.

What Information is Covered and About Whom?

The law applies to "personal information" about California residents, which is "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." The law defines such categories incredibly broadly – not only to include "normal" identifiers (e.g., name, address, Social Security Number, driver's license number), but also (among others):

- Characteristics of protected classifications under California or federal law;
- Commercial information (records of personal property, products, or services purchased, or other purchasing or consuming histories or tendencies);
- Biometric information;
- Internet information including browsing history and search history;
- Geolocation data; and
- Inferences drawn from any information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

The Substance of the Law: Individual Rights

The California law is different from the EU GDPR in at least one way, because it focuses on individual rights rather than dictating how a company must act. It provides individuals the ability to learn about a company's activities, and in turn dictate – for a particular individual – some ways in which the company can use an individual's data.

Among the key (and challenging to implement) rights are:

- 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.
- The right to request that a business delete any personal information about the consumer which the business has collected from the consumer (a right with many exceptions).
- The right to request that a business that collects personal information about the consumer disclose to the consumer a broad range of information including (1) the categories of personal information it has collected about that consumer; (2) the categories of sources from which the personal information is collected; (3) the business or commercial purpose for collecting or selling personal information; (4) the categories of third parties with whom the business shares personal information; and (5) the specific pieces of personal information it has collected about that consumer.
- The right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose

continued on page 6

(defined separately in the law), disclose to that consumer: (1) the categories of personal information that the business collected about the consumer; (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold; and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

- The right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information (what the law calls "the right to opt out"). For this right, companies must (among other things) provide "a clear and conspicuous link" on the business' Internet homepage, titled "Do Not Sell My Personal Information," to an Internet web page that enables a consumer to opt out of the sale of the consumer's personal information.

What has Happened Since the Law was Passed?

Lobbying Efforts

Not surprisingly, efforts to modify the legislation began almost immediately. A coalition of corporate entities, including the California Chamber of Commerce and many other industry associations, submitted to the legislature a formal letter seeking a variety of changes. (The letter is available **here** and **here**.) According to this coalition,

> While the full implications of the hastily passed AB 375 are far from being fully understood, in this letter, we propose amendments to address drafting errors, and to fix aspects of this bill that would be unworkable and that would result in negative consequences unintended by the authors. It is important to fix as many of these problems as soon as possible. The stakes are too high to delay any further – for consumers, businesses, the Attorney General, and the economy.

There was a consumer coalition letter submitted in response, available **here**. This coalition noted that (from its perspective) "the sky is not falling." It then summarized its concerns as follows:

> The majority of the Chamber letter's proposed changes are substantive in nature and would fundamentally water down the CCPA's privacy protections. Even when the letter does identify a provision where a technical fix is needed, the proposed solution is often excessive in nature and would run counter to the clear intention of the legislation.

The California Attorney General submitted his own letter on potential changes, available **here**. The AG expressed concern that the law imposed "several unworkable obligations and serious operational challenges" for the AG's Office, and that "failure to cure these identified flaws will undermine California's authority to launch and sustain vigorous oversight and effective enforcement of the CCPA's critical privacy protections."

Legislative Changes

Following this initial wave of lobbying, the California legislature rushed through a set of amendments (SB 1121) to the California Consumer Privacy Act before the end of the legislative session on August 31, 2018 (as of this writing, this provision has not yet been signed by the Governor).

These amendments tackled some of the ambiguities and confusion resulting from the

continued on page 7

original law. The bill expanded some of the coverage exceptions (although some of these changes may have made things even more confusing, particularly related to the health care exemption and its applicability to business associates). New exemptions were added, for example, related to clinical research subject to privacy controls under the Common Rule.

Beyond these scope exemptions, the bill addressed both enforcement and the right of consumers to sue – two of the most controversial elements of the initial law. The amendments seemed to clarify that the consumer right to sue exists only for certain data security breaches – and not more generally for violations of the "privacy" parts of the legislation. We can expect more debate on this provision.

There also were other changes related to enforcement. The requirement that a consumer notify the AG of a future lawsuit was removed. The penalty structure has been clarified. Most significantly, given the enormity of the implementation challenges and the confusion about the substance of the law, as well as the requirement (or expectation) that regulations would be issued to help explain the law, the deadline for regulations was extended and the enforcement date for the law has been pushed back until July 1, 2020.

What is Still to Come?

These amendments – assuming they are signed into law – are likely to not be the last step in the evolution of the CCPA. Like the law itself, these amendments were rushed into effect to meet a legislative deadline. Many of the provisions identified by the Chamber of Commerce letter have not been addressed at all, and we can expect significant legislative pressure to continue to revise the law. We also will see regulations from the California Attorney General about the law.

Impact on the National Debate

The California law – along with global pressure due to GDPR – has led to an increased interest at the national level in national privacy legislation. The Administration is beginning some efforts to identify a potential legislative framework. Some companies would like to see a U.S. law that would meet the European Union's "adequacy" standard. Other companies – some the same and some different – are concerned about other states that might choose to copy California's approach and see a national law with pre-emptive effect as better than a multiplicity of state laws. All of these national efforts are in their infancy.

Because of the peculiar path of the California law (the referendum initiative and the subsequent fast-track legislative process), there may be little short-term likelihood that other states will pass their own versions of the California law. Nonetheless, companies in all industries should both (1) pay close attention to the California developments, as many companies will face California compliance requirements; and (2) at the same time, become engaged in the growing national debate over national privacy legislation. Companies impacted by this law also should begin compliance preparations (although I would not move too far down the road with compliance activities just yet until some of these issues are clarified) and, in general, consider how to approach the question of whether to apply this California law on a broader national basis. ■

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Wiley Rein Launches Innovative Podcast on IoT Law and Policy

Wiley Rein LLP recently announced the launch of *Wiley Connected*, an innovative podcast exploring the fast-developing legal, regulatory, and business complexities surrounding the Internet of Things (IoT). Under the broad *Wiley Connected* umbrella, the firm will produce podcasts in a variety of lengths and formats as new or interesting issues pop up in the world of connected tech.

The most recent **episode** of Wiley Connected, "Why Tech Companies Should Care About the NDAA's New Provisions," features **Megan L. Brown**, partner in the **Telecom, Media & Technology (TMT) Practice**, who counsels clients on cybersecurity and data privacy issues; **Nova J. Daly**, senior public policy advisor in the **International Trade Practice**, who represents clients before CFIUS and on Team Telecom matters; and TMT associate **Michael L. Diakiwski**. They discuss the National Defense Authorization Act's (NDAA) provisions and recommendations, and the implications for all industries.

"As the IoT revolutionizes people's daily lives through the use of connected cars, connected health, unmanned aircraft systems, and other innovations, it has created unprecedented privacy and security challenges," said Ms. Brown, co-leader of Wiley Rein's **IoT Practice** and also a member of the firm's **Privacy & Cybersecurity**, **Appellate**, and **Litigation** practices. "We believe our podcasts will spark discussion and provide invaluable insight for clients in a range of industries."

Wiley Connected features attorneys and policy advisors from the firm's **TMT**, **Privacy & Cybersecurity**, **Unmanned Aircraft Systems (UAS)**, **Health Care**, **Insurance**, and **International Trade** practices, along with other special guests, who address a range of regulatory, litigation, and policy aspects of diverse IoT subjects. In the inaugural *Wiley Connected* episode – which aired earlier this summer – associate **Sara M. Baxenberg** and partner **Joshua S. Turner** discuss law and policy issues affecting unmanned aerial systems as part of their recurring series, "Sara and Josh Talk About Drones."

Wiley Rein is uniquely positioned to serve clients in the emerging IoT industry. The firm's **Wireless Practice**, part of the overall **TMT Practice**, is a leader in the area of connected devices, helping clients develop "bring to market," licensing, and compliance strategies for connected devices of all kinds. Wiley Rein also has extensive experience throughout its practices advocating before all federal agencies with interest in IoT, and on the Hill. Both as a thought leader and as legal counsel to companies and organizations focused on innovative technology, Wiley Rein has played a key role in shaping the discussion of emerging IoT issues and the development of IoT-related policy.

To hear recent *Wiley Connected* podcasts, please click **here**. Listeners may subscribe, rate, and leave reviews for Wiley Connected on **iTunes** and **SoundCloud**. ■

For more information, please contact:

Patricia O'Connell
202.719.4532
poconnell@wileyrein.com

Events & Speeches

Legal, Privacy and Regulatory Considerations: A Fireside Chat with Anne Kimbol

Kirk J. Nahra, Speaker

HITRUST2018

September 11, 2018 | Grapevine, TX

Cybersecurity Issues for Communications Providers

Matthew J. Gardner, Speaker

Georgetown School of Foreign Service

September 12, 2018 | Washington, DC

Trust and Privacy in the Digital Age

Kirk J. Nahra, Speaker

Washington University Law Review Symposium

September 14, 2018 | St. Louis, MO

Cybersecurity Threat to Satellites: Technology, Law & Policy

Megan L. Brown, Panelist

Intersections of Commercial and National Security Space

September 21, 2018 | Washington, DC

2nd Global Cyber Dialogue

Megan L. Brown, Panelist

U.S. Chamber of Commerce

October 10, 2018 | Washington, DC

Privacy Bootcamp

Kirk J. Nahra, Speaker

IAPP Privacy. Security. Risk. 2018

October 17, 2018 | Austin, TX

I'm a Lawyer: How Can I Advise on Data Security Issues?

Kirk J. Nahra, Moderator

IAPP Privacy. Security. Risk. 2018

October 18-19, 2018 | Austin, TX

Critical Challenges in Privacy and Security Law

Kirk J. Nahra, Speaker

Institute for Health Plan Counsel

November 2, 2018 | Chicago, IL

Mastering the Evolving Law of Data Analytics

Kirk J. Nahra, Speaker

AHIMA Data Institute: Making Information Meaningful

December 6, 2018 | Las Vegas, NV

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Michael L. Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com

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

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