Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | June 2019

This issue covers a range of important developments in privacy and cybersecurity regulation. A recent Executive Order puts restrictions on certain communications transactions in order to address cyber and national security threats, as Megan Brown, Matthew Gardner, and Daniel Brooks explain. I take a look at legislative and regulatory initiatives to mandate greater corporate board involvement in privacy and cybersecurity. We follow up on last month's deep dive on **robocalls** with the latest developments on call blocking at the FCC, written by Megan Brown, Kevin Rupy, Scott Delacourt, Kat Scott, and Boyd Garriott. And Peter Hyun and I look at recent COPPA enforcement actions on kids' privacy and ways for companies to comply.

We also include a recap of our May roundtable with FTC Commissioner Noah Joshua Phillips, which included a robust discussion of the FTC's and congressional approach to privacy. And look out for more events coming up – including a webinar on July 17 covering the latest updates on critical state privacy and security laws imposing new obligations on business. I can be reached at 202.719.4533 or **dpozza@wileyrein.com**. Thank you as always for reading.

—Duane Pozza, Partner, Privacy & Cybersecurity Practice

ALSO IN THIS ISSUE:

Foreign Telecom Deals to Be Restricted Under Sweeping New Order Targeting U.S. Network Supply Chain Security

By Megan L. Brown, Matthew J. Gardner, and Daniel P. Brooks

The technology and communications sectors are facing increasing scrutiny and regulation focused on U.S. network supply chain security in order to address what a recent Executive Order calls "malicious cyber-enabled actions" and "economic and industrial espionage." President Trump last month signed a long-anticipated **Executive Order** authorizing the Secretary of Commerce to regulate and prohibit transactions involving information and communications technology and services that are

continued on page 2

Continued from page 1

produced or supplied by "foreign adversaries." While the Order does not explicitly single out any particular country or company, it is widely believed to be aimed at Huawei and other Chinese telecommunications companies. The U.S. Department of Commerce's (Commerce) Bureau of Industry and Security (BIS) simultaneously placed Huawei and 68 of its affiliates on BIS's Entity List, prohibiting nearly all U.S. exports to them.

Long-Anticipated Executive Order Will Prohibit U.S. Companies from Buying Foreign Telecom Equipment and Services Deemed to Pose a National Security Threat

The Executive Order declares a national emergency to combat U.S. national security threats such as "malicious cyber-enabled actions" and "economic and industrial espionage." The Order, which is potentially sweeping in scope, broadly prohibits any acquisition, importation, transfer, installation, dealing in, or use of any "information and communications technology or service" where Commerce finds that "the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary," and the transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

The term "information and communications technology or services" is not limited to 5G technology and services and is defined broadly to include "any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display." The Order authorizes Commerce to issue licenses to authorize specific transactions and provides Commerce with discretion to design or negotiate mitigation measures to address any concerns "as a precondition to the approval of a transaction or of a class of transactions" that would otherwise be prohibited.

The Order directs Commerce to publish implementing regulations within 150 days of the date of the Order – i.e., by October 12, 2019 – and the National Telecommunications and Information Administration (NTIA) is expected to take a lead role. Such regulations may:

- Determine that particular countries or persons are foreign adversaries;
- Identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries;
- Identify particular technologies or countries with respect to which transactions involving information and communications technology or services warrant particular scrutiny;
- Establish procedures to license transactions otherwise prohibited pursuant to the Order;
- Establish criteria by which particular technologies or particular participants in the market for information and communications technology or services may be recognized as categorically included in or as categorically excluded from the prohibitions of the Order; and

continued on page 3

Continued from page 2

- Identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with a particular transaction.

The Executive Order also directs agencies to produce periodic assessments and reports about threats to the information and communications technology sector, and hardware, software, and services used by critical infrastructure. Federal agencies may need and seek assistance from the private sector with these assessments.

The Order is expected to particularly affect rural telecommunications operators, which tend to use Huawei network equipment due to its comparatively low cost. Recognizing that replacing Huawei equipment would be potentially cost-prohibitive for most rural carriers, a bipartisan group of Senators recently introduced the **5G Leadership Act**, which would set aside up to $700 million from future spectrum auctions to help U.S. communications providers remove Huawei equipment from their networks.

Commerce Bans U.S. Exports to Huawei

In another major blow to Huawei, BIS added Huawei and 68 of its affiliates to its Entity List, which will have considerable ramifications on the Chinese company as well as the global telecommunications industry and consumers. BIS's ban prohibits nearly all U.S.-origin exports of hardware, software, and technology to Huawei, including software and software updates/patches (unless such software is publicly available), electronic parts and components such as chips and routers, and related technology (again, unless that technology is publicly available). From a practical standpoint, users and operators may not be able to receive updates and patches for Huawei network equipment and handsets to the extent such updates or patches are provided from U.S. entities and routed through or customized by Huawei. The sweeping prohibitions also extend to the provision of parts, components, software, or other items that would be used to service or repair equipment already owned by Huawei. Additionally, foreign companies that incorporate U.S. parts and components into their products must carefully assess whether those products are subject to U.S. controls based on their U.S. content, as such products also could fall under the restrictions on Huawei.

BIS has issued a temporary general license effective through August 19, 2019, permitting the following transactions that otherwise would be prohibited:

1. ***Continued operation of existing networks and equipment*** – Companies are permitted to engage in any transactions necessary to maintain and support existing and currently fully operational networks or equipment (e.g., software updates and patches) that were subject to legally binding contracts/agreements executed between a listed Huawei entity and third parties on or before May 16, 2019.
2. ***Support*** to existing handsets – Companies also can engage in transactions necessary to provide service and support (e.g., software updates or patches) to existing Huawei phones; this provision covers models of Huawei phones that were available to the public on or before May 16, 2019.
3. ***Cybersecurity research*** and vulnerability disclosure – Companies can disclose to the listed Huawei entities information regarding security vulnerabilities in items owned, possessed, or controlled by a listed entity as part of an effort to provide ongoing security research that is critical to maintain the integrity and reliability of existing and currently fully operational networks and equipment.
4. ***Engagement as necessary*** for 5G standards by a duly recognized standards body – The temporary general license also permits

continued on page 4

Lawmakers and Regulators Are Looking at Corporate Board Involvement in Privacy and Cybersecurity

By Duane C. Pozza

As legislators and regulators consider substantive proposals to regulate how companies collect, manage, and protect consumer data, and what kind of cybersecurity protections they implement, they have increasingly looked at mandating specific steps that boards of directors must take. We have previously discussed how corporate boards are advised to **engage on cybersecurity issues**, and companies must also pay close attention to specific legislative or regulatory requirements affecting corporate board involvement. Requirements on corporate boards continue to be proposed and adopted in piecemeal fashion – particularly in the area of cybersecurity – and it remains to be seen whether they will be adopted in any federal privacy or cyber legislation. This area continues to evolve, and below we discuss a few recent actions at the state and federal level and congressional proposals that would require explicit board oversight of privacy, cybersecurity, and data governance issues, including by requiring the establishment of senior-level positions with reporting obligations directly to the board.

State Activities

States have moved forward on adopting cybersecurity regulations on a number of fronts, and some of those moves have encompassed specific requirements for corporate boards. In particular, New York and South Carolina have taken sector-specific steps on board oversight in cybersecurity.

In 2017, New York's Department of Financial Services (NYDFS) issued a cybersecurity regulation designed to address cyber threats faced by the state's financial services industry. The final regulation requires financial services institutions regulated by the NYDFS to designate a chief information security officer responsible for overseeing a mandatory cybersecurity program, with a reporting requirement to the company's board of directors or equivalent governing body.[1] The annual report must include

continued on page 5

Foreign Telecom Deals to Be Restricted Under Sweeping New Order Targeting U.S. Network Supply Chain Security; U.S. Exports to Huawei Banned

Continued from page 3

> engagement with the listed Huawei entities as necessary for the development of 5G standards as part of a duly recognized international standards body.

As national security concerns increasingly push the federal government to disrupt settled business relationships, companies must grapple with greater uncertainty in long-term planning. The challenge will be not just to understand and manage the current restrictions on Huawei, but also to be prepared for the possibility that the federal government will take actions that may fundamentally alter other aspects of the global supply chain. ▪

For additional information, please contact:

Megan L. Brown
202.719.7579 | mbrown@wileyrein.com

Matthew J. Gardner
202.719.4108 | mgardner@wileyrein.com

Daniel P. Brooks
202.719.4183 | dbrooks@wileyrein.com

Lawmakers and Regulators Are Looking at Corporate Board Involvement in Privacy and Cybersecurity

Continued from page 4

an assessment of material cybersecurity risks. New York's preeminence as an international financial hub greatly extends the reach of the NYDFS regulation.

Similarly, South Carolina took the lead in passing a cybersecurity law to address threats in the insurance industry. The South Carolina Insurance Data Security Act, effective January 1, 2019, mandates that any insurance carrier licensed in the state create a risk-based cybersecurity program with oversight by the company's board of directors.[2] Executive management must produce an annual report on material matters related to the cybersecurity program. For an insurance carrier operating in South Carolina, these kinds of requirements can have an effect on company operations that may impact cybersecurity even outside the state.

Federal Regulatory Action

Federal regulators also have begun to take action in certain areas. In February 2018, the U.S. Securities and Exchange Commission (SEC) issued updated guidance on cybersecurity disclosure obligations. Among other things, the SEC guidance provides that companies should disclose to investors how the board "engages with management on cybersecurity issues" and "discharge[es] its [cybersecurity] risk oversight responsibility." And the SEC "encourage[d] companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure."

The Federal Trade Commission (FTC) also has begun to scrutinize corporate governance with respect to cybersecurity in non-bank financial institutions. Recently, the FTC **proposed** revisions to its Safeguards Rule for financial institutions, modeled on the NYDFS regulations. The Safeguards Rule governs data security practices for financial institutions under the FTC's Gramm-Leach-Bliley (GLB) Act jurisdiction. The proposed revisions mirror the NYDFS mandate, requiring covered financial institutions to designate a chief information security officer with mandatory board reporting. In its **Notice of Proposed Rulemaking** (NPRM), the FTC has sought comment on whether a board should be required to certify compliance with the Rule.[3]

Federal Legislation

In addition to the state and federal regulatory efforts discussed above, federal lawmakers are considering whether to include board-specific requirements in crafting privacy and cybersecurity legislation. For example, in 2018, Sen. Ron Wyden (D-OR), ranking member of the Senate Finance Committee, released a discussion draft of a bill called the **Consumer Data Protection Act**.[4] The draft legislation aims to provide consumers with greater control over their data, and would cover companies under FTC jurisdiction that generate more than $50 million in annual revenue or store, share, or use personal information on more than 1 million consumers or consumer devices.

The draft bill would require covered entities to designate an employee responsible for compliance with the legislation and the annual submission of data protection reports to the FTC outlining in detail the entity's compliance with the legislation's technical and security safeguards. The designated employee also must directly report to an employee acting in an executive capacity, and each report must be accompanied by written compliance certifications from the company's chief executive officer, chief privacy officer, or chief information security officer. The draft bill would levy significant civil and criminal penalties for knowing or intentionally false certifications – executives could be "fined not more than $5,000,000 or 25 percent of the largest amount of annual compensation the person received during the previous 3-year period from the covered entity, imprisoned not more than 20 years, or both."

Additionally, the House and the Senate are considering requiring publicly traded companies to disclose whether they have cybersecurity expertise

continued on page 6

Continued from page 5

in their board of directors. On March 1, a bipartisan group of Senators reintroduced the Cybersecurity Disclosure Act, **S.592**, followed by a House companion bill, **H.R. 1731**. The bills would require publicly traded companies to include in their SEC disclosures to investors information on whether any member of the company's board is a cybersecurity expert, and if not, why having this expertise on the board of directors is not necessary because of other cybersecurity steps implemented by the company.

As the legislative process plays out in this Congress, we will be continuing to watch whether proposals to impose specific board-level obligations gain traction.

Conclusion

As lawmakers and regulators continue to evaluate whether to impose additional privacy and cybersecurity requirements, it is clear that many are seeking to elevate the importance of those issues in the company by explicitly requiring board involvement or review. Companies must pay close attention to developments in this area occurring throughout government.

Wiley Rein's Cybersecurity and Data Governance team regularly helps clients manage risk and assess compliance obligations, and we assist boards of directors and senior management in discharging their responsibilities. ▪

For additional information, please contact:

Duane C. Pozza
202.719.4533 | dpozza@wileyrein.com

NOTE: Tawanna Lee, a 2019 Wiley Rein summer associate, co-authored this article with Mr. Pozza.

Endnotes

[1] 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies § 500.04(a).

[2] *See* H.B. 4655, 122nd Gen. (S.C. 2018).

[3] 16 CFR § 314 (Apr. 4, 2019).

[4] Consumer Data Protection Act, SIL18B29, 115th Cong. § 2 (2018).

Robocall Blocking: The FCC Moves Forward and Seeks Further Comment

By Megan L. Brown, Kevin G. Rupy, Scott D. Delacourt, Kathleen E. Scott, and Boyd Garriott

On June 6, 2019, the Federal Communications Commission (FCC or Commission) unanimously[1] voted to adopt a ***Declaratory Ruling and Further Notice of Proposed Rulemaking*** on robocalls.

- The Declaratory Ruling, which became effective upon its release on June 7, expands the ability of voice providers to block certain categories of robocalls, specifically, authorizing – but not requiring – voice service providers to offer to consumers programs that (1) block unwanted calls using reasonable analytics (referred to by the FCC as "call-blocking programs") and (2) block calls from numbers not in a consumer's contact list (referred to by the FCC as "white-list programs"). The Declaratory Ruling authorizes the first category – call-blocking programs – on an opt-out basis, and the second category—white-list programs – on an opt-in basis.
- The ***Further Notice of Proposed Rulemaking (FNPRM)*** considers (1) establishing safe harbors for voice providers engaged in certain types of call blocking; (2) adopting safeguards to ensure public safety calls are unimpeded by such blocking; (3) mandating SHAKEN/STIR for certain voice service providers if those providers do not voluntarily implement SHAKEN/STIR by the end of the year; and (4) creating a mechanism to measure the effectiveness of robocall solutions.
- Additionally, the item calls for two new robocall reports from FCC staff.

Comments in response to the *FNPRM* will be due 30 days after publication of the item in the *Federal Register*.

The following summarizes the items adopted by the FCC and highlights significant changes between the **draft release** (summarized **here**) and the final version adopted by the Commission.

The *Declaratory Ruling* Expands Voice Service Provider Authority to Offer Call-Blocking Programs on an Opt-Out Basis, but Does Not Create a Corresponding Safe Harbor.

The FCC's *Declaratory Ruling* permits – but does not require – voice service providers to offer call-blocking programs to customers on an opt-out basis. While this action expands authority for call blocking, it does not establish a safe harbor for such blocking, and at the same time, it imposes various parameters on call-blocking programs. In addition to the four parameters outlined in the *Draft Declaratory Ruling*, the FCC added a fifth parameter to address instances of inappropriate blocking of legitimate calls. This parameter requires providing a point of contact to call originators to resolve such instances (as well as a mechanism to do so), and encourages voice service providers to provide a mechanism to notify call originators that their calls have been blocked (discussed below). This parameter did not appear in the *Draft Declaratory Ruling*.

The FCC notes that while blocking tools are currently available to consumers, they are often provided on an opt-in basis, which it concludes "limit[s] the impact of such programs on consumers." ¶ 27. The FCC also reiterates the absence of any "legal dispute in the record that the Communications Act or Commission rules do not limit consumers' right to block calls, as long as the consumer makes the choice to do so." ¶ 31. It further concludes that "opt-out call-blocking programs are generally just and reasonable practices (not unjust and unreasonable practices) and enhancements of service (not impairments of service)." ¶ 31.

The adopted item outlines five parameters of its ruling regarding opt-out call-blocking programs. The first four parameters were previewed in the draft item (although changes were made in the version that was adopted); the fifth parameter – dealing with

continued on page 8

Continued from page 7

concerns of erroneous blocking – was not in the *Draft Declaratory Ruling*.

1. The Commission clarifies that "voice service providers offering opt-out call-blocking programs must offer **sufficient information so that consumers can make an informed choice** as to whether they wish to remain in the program or opt out." ¶ 33. Examples include messages on a provider's website, bill inserts, e-mails, and texts. At a minimum, the FCC expects voice service providers "to describe in plain language how the call blocking-program makes the determination to block certain calls, the risks that it may block calls the consumer may want, and how a consumer may opt out of the service." ¶ 33 It also states its expectation that any opt-out process be "simple and straightforward." ¶ 33.
2. The Commission clarifies that voice service providers may base the opt-out call-blocking programs **"on any reasonable analytics designed to identify unwanted calls."** ¶ 34. It declines to adopt "rigid blocking rules," as such an approach would be easy for illegal actors to evade, and would impede the development of diverse blocking services. ¶ 34. Examples of reasonable analytics include blocking calls based on large bursts of calls in a short timeframe; low average call duration; low call completion ratios; and other criteria. The adopted item adds that "[t]o be reasonable, however, such analytics must be applied in a non-discriminatory, competitively neutral manner." ¶ 35.
3. The FCC reaffirms its commitment to **safeguard calls from emergency numbers**. In the adopted item, the FCC cautions voice service providers not to use blocking tools by default to avoid blocking calls from "public safety entities, including [Public Safety Answering Points (PSAPs)], emergency operations centers, or law enforcement agencies." ¶ 36. It also urges providers to "make all feasible efforts for those tools to avoid blocking emergency calls." ¶ 36
4. The FCC also reaffirms its commitment to **safeguard calls to rural areas**. The agency does not anticipate that its determination will negatively impact rural call completion rates, since call-blocking programs would be offered by the terminating providers. However, the item reminds voice service providers that call-blocking programs "may not be used to avoid the effect of our rural call completion rules." ¶ 37.
5. Finally, the Commission addresses "concern about blocking of calls required for compliance with other laws, rules, or policy considerations" by including a final parameter that holds that **"a reasonable call-blocking program instituted by default would include a point of contact for legitimate callers to report what they believe to be erroneous blocking as well as a mechanism for such complaints to be resolved."** ¶ 38. The Commission further indicates that **"callers who believe their calls have been unfairly blocked may seek review of a call-blocking program they believe to be unreasonable by filing a petition for declaratory ruling with the Commission."** ¶ 38. Noting that "industry has been active in developing solutions that allow callers to communicate with voice service providers and analytics companies to identify themselves and share their call patterns that might otherwise seem to indicate illegal call activity," the Commission further encourages voice service providers to develop a mechanism for notifying callers that their calls have been blocked. ¶ 38.

The *Declaratory Ruling* Also Permits an Opt-In White List Approach for Call Blocking.

In addition to permitting robocall blocking programs to consumers on an opt-out basis, the *Declaratory Ruling* makes clear that nothing in the Act or the

continued on page 9

Continued from page 8

FCC's rules "prohibits a voice service provider from offering an opt-in white list program using the consumer's contact list." ¶ 46. This approach would block all calls to the consumer, except for those contained on the customer-defined white list. Such offerings could only be offered on an opt-in basis, and the FCC notes that voice service providers "should clearly disclose to consumers the risks of blocking wanted calls and the scope of information disclosed in a manner that is clear and easy for a consumer to understand." ¶ 46.

The *FNPRM* Seeks Comment on Proposals for Narrow Call Blocking Safe Harbors.

In the *FNPRM*, the Commission proposes a "narrow safe harbor for blocking in specific instances based on SHAKEN/STIR." ¶ 49. Specifically:

- The FCC proposes a "**safe harbor for voice service providers that choose to block calls (or a subset of calls) that fail Caller ID authentication under the SHAKEN/STIR framework,"** noting that "call-blocking programs that consider the degree of attestation (whether full, partial, or gateway attestation) for successfully authenticated calls would not fit within the scope of this safe harbor" and that "only calls for which attestation information is available – the originating provider has implemented SHAKEN/STIR and each intermediate provider in the call path accurately passes authentication information to the terminating provider – and that fail authentication would be blocked." ¶¶ 51-53.
- The FCC seeks comment on whether it should establish a "**safe harbor for blocking unsigned calls from "particular categories of voice service providers."** ¶ 54. Such categories include voice providers participating in the SHAKEN/STIR framework that fail to sign certain calls, as well as certain "larger voice service providers." ¶ 54. The FNPRM asks whether the safe harbor should apply to calls from a large service provider that fails to implement the SHAKEN/STIR standards by a certain timeframe. It also seeks comment on how to define "large voice service provider." Alternatively, the FNPRM asks whether a safe harbor should target voice service providers that are most likely to facilitate unlawful robocallers. For example, pointing to the USTelecom Industry Traceback Group, it asks whether a safe harbor should target those voice service providers that do not appropriately sign calls *and* do not participate in the Industry Traceback Group. With respect to smaller providers, the FCC also seeks comment on how it can ensure that any safe harbor does not impose undue costs on eligible telecommunications carriers participating in the agency's high-cost program.

Additionally, the FNPRM seeks comment on whether particular protections should be established for a safe harbor "to ensure that wanted calls are not blocked." ¶ 58. It asks whether it should require voice service providers seeking a safe harbor to provide a mechanism for identifying and remedying the blocking of wanted calls or to send an intercept message or other indication that a call has been blocked. The FCC also seeks comment on how its proposal intersects with the agency's recently adopted rural call completion rules.

Finally, in the section related to safe harbors, the adopted item adds a discussion of the use of SHAKEN/STIR analytics. Specifically, the Commission notes that "SHAKEN/STIR's ability to determine the source of robocalls will be a significant contribution to the quality of [] analytics," and asks (1) how it can "best promote the use of SHAKEN/STIR-based analytics;" and (2) "[w]hat steps should [the FCC] take to encourage or require the use of SHAKEN/STIR-based analytics." ¶ 62.

continued on page 10

Continued from page 9

The *FNPRM* Also Seeks Comment on Proposals for a Critical Calls List

The FCC considers "requiring any voice service provider that offers call-blocking to maintain a 'Critical Calls List' of numbers it may not block." ¶ 63. It seeks comment on which numbers should be required on a Critical Calls List (such as PSAPs and government emergency outbound numbers) and whether the list should be expanded to include calls from other organizations such as schools, doctors, local governments, or alarm companies, or certain other types of calls, such as fraud and weather alerts. The FCC also seeks comment on:

- whether such a list should be centrally maintained (and if so, by whom), or whether each voice provider should maintain its own list;
- whether the Critical Calls List protections should be limited to authenticated calls;
- whether the list should be made public, and if not, which entities should be authorized to access the list;
- whether voice providers should ever be permitted to block numbers contained on the list;
- the costs and benefits associated with implementing the list; and
- whether mechanisms exist that would enable blocking of illegal spoofed calls to PSAPs without blocking legitimate 911 calls.

The *FNPRM* Proposes a SHAKEN/STIR Mandate If Major Voice Service Providers Have Not Implemented the Caller ID Authentication Framework by the end of 2019.

The *FNPRM* seeks comment on the proposal to mandate SHAKEN/STIR if "major voice service providers fail to meet an end of 2019 deadline for voluntary implementation." ¶ 71. This proposal was not in the draft item. Noting the progress of many providers towards implementation, the FCC discusses the importance of implementing the framework across voice networks. Under this proposal, the FCC asks, among other things:

- How to define "major voice service provider;"
- How to evaluate whether major voice service providers have met the end-of-year implementation deadline; and
- Whether to require certifications of compliance.

Additionally, the FCC asks a series of questions about the SHAKEN/STIR mandate, *if* the Commission needs to issue a mandate. Among other questions, the Commission asks:

- Whether to require implementation by all voice service providers – wireline, wireless, and Voice over Internet Protocol (VoIP) providers;
- What it should require providers to accomplish to satisfy the mandate, including questions about adopting displays;
- How much implementation time is needed for voice service providers;
- What role the Commission should have in SHAKEN/STIR governance; and
- "[H]ow to encourage Caller ID authentication for carriers that maintain some portion of their network on legacy technology." ¶ 80.

Finally, the Commission asks how it can leverage SHAKEN/STIR to address illegal calls that are originated outside of the United States.

The *FNPRM* Asks About Measuring the Effectiveness of Robocall Solutions.

In this new section added since the draft version of the item was circulated, the Commission asks both whether and how it could "create a mechanism to provide information to consumers about the effectiveness of various voice service providers' robocall solutions." ¶ 83.

continued on page 11

Continued from page 10

The Commission Calls for Two New Robocall Reports.

Additionally, with this item, the Commission calls for FCC staff "to prepare two reports on the state of deployment of advanced methods and tools to eliminate such calls, including the impact of call blocking on 911 and public safety." ¶ 87. The FCC's adopted framework for the reports follows a 2017 recommendation from the Consumer Advisory Committee, and the first and second report are due to the agency 12 months and 24 months, respectively, from the date of publication of the *Declaratory Ruling* and *FNPRM* in the Federal Register. The FCC also delegates authority to the Consumer and Governmental Affairs Bureau, in consultation with the Wireline Competition Bureau and Public Safety and Homeland Security Bureau, to collect "any and all relevant information and data from voice service providers necessary to complete these reports." ¶ 90. ▪

For additional information, please contact:

Megan L. Brown
202.719.7579 | mbrown@wileyrein.com

Kevin G. Rupy
202.719.4510 | krupy@wileyrein.com

Scott D. Delacourt
202.719.7459 | sdelacourt@wileyrein.com

Kathleen E. Scott
202.719.7577 | kscott@wileyrein.com

Boyd Garriott
202.719.4487 | bgarriott@wileyrein.com

ENDNOTE

[1] Commissioners O'Rielly and Rosenworcel voted to adopt both items, but dissented on discrete aspects of each.

Cybersecurity Law Report
An Acuris company

cslawreport.com

June 19, 2019

COPPA

Kids, Privacy & Legal Compliance

By Peter S. Hyun and Duane Pozza, *Wiley Rein*

It is estimated that every day more than 2,500 apps are added to the Apple App Store, and more than 1,300 to the Google Play Store. These staggering figures reflect a virtual marketplace where app developers are under significant pressure to be the first to market, to "disrupt" industries and/or to be the first to innovate a new market. However, rushing to market without first devoting time and resources to legal compliance can pose significant business risk for companies down the road. One area where it is important to ensure compliance early on is the protection of children's privacy.

See "COPPA Compliance Lessons Following Musical.ly's $5.7 Million FTC Settlement" (Mar. 20, 2019).

The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA), enacted in 1998, requires online service providers that direct services to children (under age 13) and collect personal information from children to protect children's data, provide a clear privacy notice to users and parents and get parental consent before collecting certain information from kids.

While COPPA vests broad regulatory and enforcement authority with the FTC, COPPA also affords State Attorneys General with authority to enforce COPPA. Both the FTC and State Attorneys General across the country have been extremely active in enforcing COPPA in recent years, particularly in the wake of data breaches and sweeping new privacy laws in the European Union and California.

See CSLR's three-part series analyzing early GDPR enforcement: "Portugal and Germany" (Jan. 23, 2019); "U.K. and Austria" (Jan. 30, 2019), "France" (Feb. 6, 2019); and "CCPA Priorities: Turning Legislation Prep Into a Program Shift" (Jun. 5, 2019).

Recent COPPA Enforcement Actions

Several months ago, the New York Attorney General's office reached a $5-million settlement with a large online media company to resolve allegations that the company's online advertising business was unlawfully targeting display ads on websites it knew were directed at children. New York and other states have brought a variety of enforcement actions against online companies over the past decade.

The FTC has also been active in COPPA enforcement. Earlier this month, three online dating apps were removed from Apple's App Store and the Google Play store after the FTC alleged those apps allowed children to access them in violation of COPPA. Not only did the FTC issue a warning letter to the apps, but it also issued a consumer alert for parents regarding the dating apps.

These stern consumer alerts followed a series of notable FTC COPPA settlements with website operators under various provisions in COPPA. In April, the FTC settled a COPPA case against a dress-up games website that included allegations under the data security provision of COPPA. That provision requires operators to take reasonable steps to safeguard consumer data. The vulnerabilities on the website allowed hackers to breach the platform, putting millions of consumers' data at risk.

The FTC also resolved another COPPA investigation – the largest ever – with a prominent video social networking app with over 200 million users. The $5.7-million settlement resolved allegations that the video app illegally collected personal information from children and failed to seek parental consent before collecting kids' private information.

The dress-up website settlement and video app settlement also involved coordination with the Consumer Protection section of the U.S. Department of Justice. In the video app settlement, for example, the Justice Department and the FTC jointly filed a federal court consent decree that bound the company to comply with COPPA going forward, and take down all videos made by children under the age of 13. This type of coordination between the FTC and the Justice Department is not uncommon.

See also "Lessons From FTC 2018 Privacy and Data Security Update: Financial Privacy, COPPA and International Enforcement" (May 1, 2019).

COPPA Reforms and Policymakers

Not only do government enforcers have COPPA squarely on their radar but policymakers do as well. In the Internet of Things era, and with the ubiquitous nature of online services and activity, much has been made about efforts to update the 20+ year old COPPA law to match technological advancements.

Recently, Senators Ed Markey (D-MA) and Josh Hawley (R-MO) have pressed for changes to COPPA to extend even greater data privacy protections to children. The bipartisan duo recently introduced a bill that would update COPPA to require that online companies create an erase button for parents to remove all of their child's data from a service.

These types of policy proposals follow a sweeping change that the FTC undertook at the end of 2012 with respect to how the Commission defined critical terms within COPPA. The FTC modified, for example, key definitions such as what comprised "personal information" and "website or online service directed to children," and also revised notice requirements and consent mechanisms under the statute. The updates were made because of calls to stay current "amidst whirlwind technological change."

Additionally, just weeks ago, the Chinese government, through its top internet regulator (the Cyberspace Administration of China), released draft COPPA-like regulations applicable to online providers. The draft regulation would cover the collection of personal information relating to children under age 14. The draft shares many similarities with COPPA – including parental consent provisions and consumer disclosure provisions – but it also incorporates additional security requirements such as data breach notification requirements and encryption requirements. Undoubtedly, stakeholders will be carefully attentive to the final implementation of the regulation in China.

How Can You Achieve COPPA Compliance?

With COPPA compliance being a hot issue for regulators, enforcers and policymakers, it is incumbent on all online companies – including app developers – to incorporate an appropriate COPPA/privacy compliance strategy into its business plan early on.

Indeed, before a product or service is launched, it is essential to have at least a baseline understanding of how to deal with future government risk and/or investigations in this area. Assessing that risk, however, can be difficult, given the complex policy and regulatory environment that many tech companies operate under, and given the nuances that each product or service possesses on its own.

Taking a proactive approach early on to issue-spot legal risk and COPPA compliance before deploying a new product or service can help minimize potential violations and the cascade of troubles that can follow. Ensuring compliance at the beginning of the development process can also help preserve a compliance culture that can serve the company well long into its future.

The FTC has a helpful six-step compliance plan for COPPA, and the following are additional considerations to think through when putting together a plan for COPPA compliance in the context of a broader assessment of privacy, cybersecurity and data governance risks.

See "Focus on Children's Privacy by FTC and Plaintiffs Calls for Prioritizing COPPA" (Sep. 13, 2017).

Create a Risk-Management Plan

As a general matter, every business must assess data-related risks and prioritize them to determine how it will manage risk events as they arise. When thinking through a COPPA risk-management plan, consider that it encompasses sensitive private data of children and, thus, risk in this area goes beyond legal risk to include, among other things, reputational risk and political risk. Therefore, developing a plan to identify areas in which children's data may be gathered and COPPA obligations may be triggered, assess compliance obligations, and manage risks related to such data is of utmost importance.

Conduct an Internal Review of Your Product

Not only should the business have a clear view of the legal COPPA requirements (through help with outside counsel or otherwise), but early on, when a company is designing its product or service, the company should evaluate whether and how it may be used by children under the

age of 13. If, in fact, it may be used by children, conducting an internal review can help the company clearly determine what kind of data it collects, as well as how that data is used, stored, shared, and accessed, and whether any changes should be made for COPPA compliance purposes. Commonly, companies will create and analyze data flow maps to help understand these points. And, at a minimum, where companies have actual knowledge of customers' ages under 13, companies must pay close attention to ensure they are satisfying all applicable COPPA requirements.

Develop Clear and Consistent Privacy Policies

It is important that your consumer-facing privacy policy corresponds with privacy and data security policies and procedures that apply internally across the company, across all components and sectors. In other words, policies should not just apply to IT departments, but across the organization. Policies should also include designated personnel to train and enforce on data governance policies.

Secure Data

Companies should be mindful of securing their own data, particularly where the data may be accessed or provided to a third party. Companies should carefully review data security provisions in third-party contracts, and in doing so, implement contractual commitments to ensure compliance with COPPA, the company's privacy and data security policies and other legal obligations that may apply.
Given the regulatory and enforcement environment on issues of privacy and data security, companies should strongly consider COPPA compliance early on in their product or service life cycle and take steps to avoid COPPA-related headaches down the road.

See CSLR's two-part series on how to maintain effective and secure long-term vendor relationships: "Understanding the Risks" (Jun. 20, 2018); "Addressing the Issues" (Jun. 27, 2018).

Peter S. Hyun, a partner at Wiley Rein LLP, represents individuals and entities in government enforcement actions, congressional investigations and State Attorneys General investigations. He is a former Assistant U.S. Attorney in the Eastern District of Virginia's U.S. Attorney's Office, Assistant Attorney General in the New York Attorney General's office and Chief Counsel to U.S. Senator Dianne Feinstein on the U.S. Senate Committee on the Judiciary.

Duane C. Pozza, a partner at Wiley Rein LLP, counsels on tech regulation, consumer protection and FTC enforcement. He advises clients on key legal issues, advocacy positions and regulatory compliance involving consumer uses of developing technology. Prior to joining Wiley Rein, Pozza was an Assistant Director in the Division of Financial Practices at the FTC's Bureau of Consumer Protection, where he led consumer protection efforts in financial technology and other sectors, and supervised investigations and enforcement actions involving consumer protection issues on technology platforms.

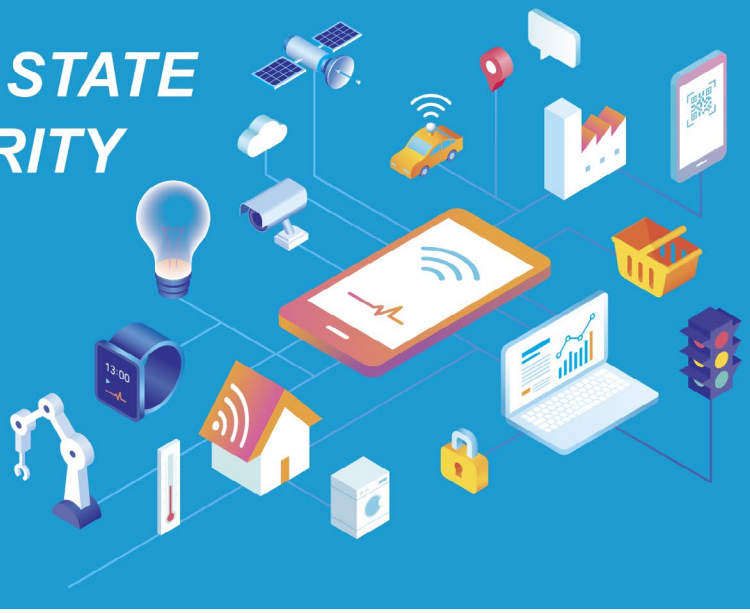
Roundtable with FTC Commissioner Phillips Recap

On May 16, Wiley Rein hosted FTC Commissioner Noah Joshua Phillips for a roundtable discussion, moderated by partner Duane C. Pozza. Commissioner Phillips discussed a range of topics, including consumer data privacy enforcement and potential legislation, remedies for privacy and data security violations, and the FTC's approach to artificial intelligence (AI) and other emerging technologies.

Among other points, Commissioner Phillips explained his view that consumer data privacy efforts should be directed at specific harms that warrant a remedy. And in discussing potential federal legislation, he emphasized that tools like penalties and rulemaking should be calibrated carefully to address harms that Congress identifies. He also noted that Congress should weigh the trade-offs involved in new regulation, and make fundamental value judgments itself rather than delegating expansive rulemaking authority to the FTC.

Commissioner Phillips was confirmed as one of five Commissioners in April 2018 and sworn in on May 2, 2018. His term extends until September 2023.

LATEST UPDATE ON STATE PRIVACY AND SECURITY LAWS: CALIFORNIA AND BEYOND



WEBINAR | July 17, 2019 @ 2 PM (EDT)

States from California to Maine continue to be active in considering and passing legislation governing data privacy and security. In California, legislators have been busy considering amendments to the California Consumer Privacy Act. Other states like Oregon, Maine, and Nevada have recently passed their own laws. All of these laws will significantly affect how businesses collect, use, share, and protect data. Join us to discuss the latest developments and practical tips on how to navigate compliance obligations even as the legal landscape around data privacy continues to evolve.

RSVP

For more information, please contact: Abby Reyes
202.719.4498 | areyes@wileyrein.com

Matthew J. Gardner
Partner
mgardner@wileyrein.com
202.719.4108

Duane C. Pozza
Partner
dpozza@wileyrein.com
202.719.4533

Kathleen E. Scott
Associate
kscott@wileyrein.com
202.719.7577

Joan Stewart
Of Counsel
jstewart@wileyrein.com
202.719.7438

Events & Speeches

A Discussion on Cybersecurity & Privacy Policy
The Women's High-Tech Coalition and the Women's High-Tech Caucus
Megan L. Brown, Speaker
June 11, 2019 | Washington, DC

The Legal Ethics of Email and Social Media
The American Health Lawyers Association
Dorthula H. Powell-Woodson, Speaker
June 24, 2019 | Boston, MA

At the Intersection of Digital innovation and Privacy: The Impact of State Privacy Regulations
FMI Legal and Regulatory Compliance Conference
Matthew J. Gardner, Speaker, Joan Stewart, Speaker
June 25, 2019 | Charleston, SC

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

5G, Huawei, and National Security
Wiley Rein National Security Webinar + Podcast Series
Megan L. Brown, Speaker
September 12, 2019

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
Bethany A. Corbin	202.719.4418	bcorbin@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
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.