Before we begin

Tech Support

If you are experiencing technical difficulties, please contact WebEx Tech Support at +1.866.779.3239.

Q&A

The Q&A tab is located near the bottom right-hand side of your screen; choose "All Panelists" before clicking "Send."

CLE

We will mention a code at some point during the presentation for attendees who requested CLE. Please make note of that code, and insert it in the pop-up survey that will appear in a new browser tab after you exit this webinar. You will receive a Certificate of Attendance from our CLE team in approximately 30 to 45 days.

Audio

The audio will remain quiet until we begin at 2:00 pm ET.

You will hear sound through your computer speakers/headphones automatically. Make sure your speakers are ON and UNMUTED.

To access the audio by telephone, please click the "phone" icon below your name on the Participants Panel for teleconference information.

Morgan Lewis

TECHNOLOGY MARATHON

Hot Privacy and Data Security Issues on the Hill and at the FCC and FTC

Greg Parks and Ron Del Sesto

Tuesday, May 23

Presenters

Gregory T. Parks

Ronald W. Del Sesto, Jr.

Morgan Lewis

The Federal Communications Commission

Morgan Lewis

Federal Communications Commission (FCC)

- Typically composed of five Commissioners (maximum of three can be from one political party, including Chair)
- Commissioners nominated by President and confirmed by Senate
- Commissioners have staggered, five-year terms (except when filling an unexpired term)
- FCC Chair appoints staff and controls agenda; first among equals

FCC Commissioners

Jessica Rosenworcel (D), term expires 6/30/2025

- Second appointment as Commissioner
- Named to serve as Acting Chair in January 2021
- Designated permanent Chair in October 2021 and confirmed by Senate as Chair in December 2021

Geoffrey Starks (D), term expires 6/30/2023

- Confirmed by Senate in January 2019
- Former prosecutor with experience in FCC Enforcement Bureau

Brendan Carr (R), term expires 6/30/2023

- Former advisor to FCC member Ajit Pai, briefly served as General Counsel of FCC

Nathan Simington (R), term expires 6/30/2024

- Former senior advisor at NTIA

Open seat

Net Neutrality

- In 2015, the Democratic-led FCC classified broadband as a Title II telecommunications service, giving the FCC more regulatory authority over broadband service providers
  - The FCC also laid out three bright-line net neutrality rules that prohibited broadband service providers from blocking or throttling legal internet traffic or prioritizing certain traffic for payment
- In 2018, under Republican leadership, the FCC repealed the 2015 order, classifying broadband as a Title I information service and eliminating the FCC's authority to impose Net Neutrality rules
  - Internet service providers were required to publicly disclose if traffic is blocked, throttled, or prioritized — though operators are not prohibited from those activities
- Under Chair Rosenworcel and a majority Democrat FCC we would expect the FCC to look to reinstate provisions of the 2015 order, reclassify broadband service as telecommunications service, and reestablish greater authority over broadband service providers

Net Neutrality (cont'd)

- The road to new net neutrality order likely to take a year or more, and FCC expected to need time to assemble factual record and develop legal analyses to reinstate, in essence, the 2015 order
- A new net neutrality order likely to bring back 2015 "bright line" rules and move to classify internet service providers as Title II carriers (subject to common carrier regulations, including enforcement)
  - No blocking – no blocking of lawful content, applications, services, or nonharmful devices
  - No throttling – cannot impair or degrade lawful internet traffic on the basis of content, application, or service, or use of a nonharmful device
  - No paid prioritization – prohibited from managing a broadband network to, directly or indirectly, favor some traffic over other traffic (a) in exchange for consideration (monetary or otherwise) from a third party, or (b) to benefit an affiliated entity
  - "No blocking" and "no throttling" rules subject to reasonable network management exception – practices primarily used for and tailored to achieving a legitimate network management purpose, but not for other business purposes

Net Neutrality (cont'd)

Under Title II, the FCC would technically have the authority to impose rate regulation and force unbundling

However, the FCC is unlikely to institute new Net Neutrality requirements that extend beyond the scope of the 2015 order (which employed a "light-touch" approach for the use of Title II)

- No rate regulation,
- No unbundling of last-mile facilities,
- No tariffing,
- No cost-accounting rules, and
- No new federal taxes or fees

Appeal guaranteed

- FCC will need to justify reversing its 2018 order and explain to the DC Circuit why the court's rationale that upheld the 2018 order's classification of broadband internet services as an "information service" under Title I allows the FCC to reclassify the broadband services as a "telecommunications service"
- DC Circuit may suffer from net neutrality fatigue–third order on appeal since 2015
- Court may question providing the FCC *Chevron* deference given fluctuating decisions
- No guarantee that DC Circuit will agree with the FCC's second attempt at applying Title II, and legislation may be needed to institute Net Neutrality safeguards

Additional Policy Initiatives

- National Security
  - The FCC continues with efforts to ensure integrity of telecommunications and internet network infrastructure and to address national security threats
  - Anti-Chinese measures focused on carriers, apps, equipment manufacturers, and submarine cables continues into Biden Administration (e.g., Infrastructure Investment and Jobs Act)
- Enforcement
  - Enforcement initiatives associated with finding and remedying "waste, fraud, and abuse" of USF funds expected to continue
  - Investigations of E-Rate and Rural Healthcare have been proceeding unabated
  - Biden FCC has been aggressive on ensuring accuracy of carrier reports

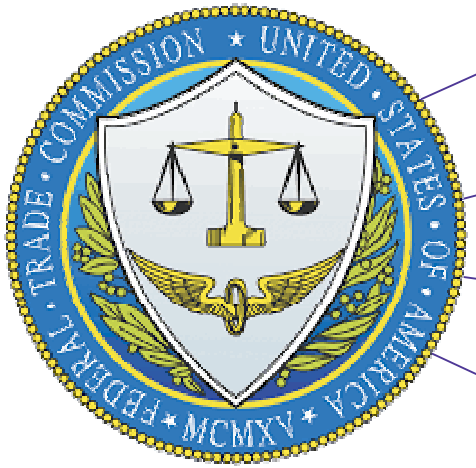
Section 230 of the Communications Decency Act

- Calls for reform of Section 230 have increased
- While criticism of Section 230 has come from both sides of the political aisle, Democrats and Republicans are not unified in their concerns
  - Democrats say too much hate, election meddling, and misinformation gets posted online
  - Republicans claim their ideas and candidates are censored
- Uncertain whether the FCC has the authority to interpret Section 230
- The FCC most likely will continue to defer to Congress
- U.S. Supreme Court recently resolved a pair of cases testing Section 230 liability protections
- Section 230 and Artificial Intelligence

THE FEDERAL TRADE COMMISSION

Morgan Lewis

Federal Trade Commission (FTC)



- Led by five Commissioners nominated by the President and confirmed by the Senate
- Each serves a seven-year term
- No more than three Commissioners can be from the same political party
- President selects one Commissioner to act as Chair

FTC Commissioners

Lina M. Khan (D) – Chair and sworn in June 15, 2021

Rebecca Kelly Slaughter (D) – Commissioner and sworn in May 2, 2018

Alvaro Bedoya (D) – Commissioner and sworn in May 16, 2022

FTC's Focuses on Artificial Intelligence

- Apr. 25, 2023 –Joint Statement on AI
- Feb. 17, 2023 – Launch of Office of Technology
- Aug. 11, 2022 – Commercial Surveillance and Data Security ANPRM
- June 16, 2022 – FTC Report Warns About Using AI to Combat Online Problems
- Apr. 19, 2021 – Aiming for truth, fairness, and equity in your company's use of AI
- Nov. 19, 2021 – Chair Lina Khan announces new additions to OPP
- Apr. 8, 2020 – Using Artificial Intelligence and Algorithms
- Nov. 2018 – FTC Hearing #7: The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics
- Jan. 2016 – Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues

ANPRM on Commercial Surveillance & Data Security

- Comment deadline closed November 21, 2022
- Purports to pursue new privacy and data security regime
  - Transcends consumer privacy
  - Overhaul of the regulatory landscape governing numerous facets of the US economy
- Includes 95 questions

ANPRM Impact

- Procedurally interesting
  - Magnuson-Moss rulemaking or process
  - FTC must also submit the proposal to its oversight committees in Congress, at least 30 days prior to publishing of the proposed rule
  - Hearing component
  - Enhanced judicial review

Updating Rulemaking Procedures

- July 1, 2021 – FTC party-line vote to "update" rulemaking procedures
  - Partially in response to *AMG Capital Management v. FTC*
  - "Streamlined" procedures for Section 18 rules
  - Eliminated requirements not imposed by the FTC Act
  - Dissent of former Republican Commissioner Christine S. Wilson

FTC Report "Bringing Dark Patterns to Light"

- FTC Releases Report on Dark Patters (Sept. 15, 2022)
  - Commission voted 5-0 to authorize release of the report
  - "Design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm"
    - Design elements that induce false beliefs
    - Design elements that hide or delay disclosure of material information
    - Design elements that lead to unauthorized charges
    - Design elements that obscure or subvert privacy choices

Protecting Children's Privacy

- Protecting Children's Privacy
  - Chegg Inc. (final order Jan. 27, 2023; voted 4-0 to pursue the complaint on Oct. 31, 2022)
    - Alleged that Chegg failed to protect PI collected from its users and employees
    - Alleged that the failure led to four data breaches dating back to 2017
    - Alleged that it failed to implement basic security measures, stored information insecurely and did not develop adequate security policies and training
    - Requires Chegg to (1) detail and limit data collection; (2) provide consumer access to data; (3) offer multifactor authentication; and (4) implement security program
  - Epic Games (Dec. 19, 2022)
    - Alleged company collected children's PI without obtaining parents' verifiable consent; requests to delete children's PI imposed unreasonable process; use of dark patterns
    - $520 million in relief – two components: (1) $275 million for violation of COPPA Rule; and (2) $245 million in refunds to consumers
    - Imposes requirement addressing default privacy settings

Protecting Children's Privacy (cont'd)

- Protecting Children's Privacy
  - FTC Policy Statement on Education Technology and COPPA (May 19, 2022)
    - Prohibits mandatory collection as condition in any activity
    - Restricts use of PI collected from children
    - Retention prohibition
    - Imposes security requirements to maintain confidentiality, security, and integrity of PI

Other FTC Enforcement Actions

- FTC's Authority to Provide Monetary Relief to Consumers
  - *AMG Capital Management v. FTC* – Supreme Court ruled that Section 13(b) of the FTC Act does not authorize federal courts to require defendants to pay refunds or forfeit "gains"
  - FTC used this provision from 2016 to 2022 to obtain $11.2 billion in a broad range of cases, including data security and privacy, telemarketing fraud, anticompetitive pharmaceutical practices, and scams targeting seniors and veterans
  - April 28, 2022 – Chair Khan joins Commissioner Slaughter's statement calling for the Senate to pass legislation restoring the FTC's ability to obtain monetary relief pursuant to Section 13(b) of the FTC Act

Other FTC Enforcement Actions (cont'd)

- Data Security Action against Drizly (final order Jan. 10, 2023) 4-0 vote
  - Named CEO James Cory Rellas, in both an individual and corporate officer capacity
  - Alleged failure to maintain appropriate security safeguards
  - Requires the company to: (1) destroy unnecessary data, (2) limit the company's data collection practices to only information that is necessary for specific purposes outlined in a retention schedule, and (3) implement a comprehensive ISP establishing security safeguards to protect against security incidents (including requiring employee training, appointing a high-level employee responsible for overseeing the company's information security program, implementing data access controls, and requiring employees to use multi-factor authentication to access databases containing consumer personal information)
  - Requires CEO Rellas to implement an information security program at a *future company* that collects PI of >25,000 people
- *FTC v. Kochava, Inc*. (filed complaint on Aug. 29, 2022) in U.S. District Court for the District of Idaho
  - Alleged unlawful selling geolocation data from hundreds of millions of mobile devices that can be used to trace movements of individuals to and from sensitive locations.
  - Seeks halt the sale of such information and destruction of same.
  - May 4, 2023 – federal judge dismisses complaint

Enforcement Action Takeaways

- Focusing on Effective Remedies
  - Obtaining not only monetary penalties but injunctive relief increasingly includes destruction of data collected in violation of customer agreements and any algorithms derived from it
  - Banned a CEO and a company from the surveillance business entirely through a consent decree alleging that the company had been secretly harvesting and selling real-time access to data concerning sensitive activity

ROBOCALLING/TEXTING AND THE SHARED JURISDICTION OF THE FCC AND FTC

Morgan Lewis

FCC and FTC Share Enforcement

Laws and Regulations	Agency	Types of Calls Covered
TCPA and FCC Rules	FCC	Restricts certain calls made using an artificial or prerecorded voice to residential lines; certain calls made using an artificial or prerecorded voice or an automatic telephone dialing system to wireless telephone numbers; and certain telemarketing calls.
2009 Truth in Caller ID Act	FCC	Prohibition on the knowing transmission of misleading or inaccurate Caller ID information "with the intent to defraud, cause harm, or wrongfully obtain anything of value."
Do Not Call Implementation Act	FTC, FCC	Authorizes the FTC to collect fees for the implementation and enforcement of a Do Not Call Registry. Telemarketers must consult the National Do Not Call Registry before calling. Requires that "the [FCC] shall consult and coordinate with the [FTC] to maximize consistency with the rules promulgated by the [FTC]."
Telemarketing Consumer Fraud and Abuse Prevention Act and Telemarketing Sales Rule	FTC	Prohibits deceptive and abusive telemarketing acts or practices.

Robocalling and Key Developments

- The Supreme Court's decision in *Barr v. American Association of Political Consultants Inc.* invalidating the government-debt exception to the TCPA as unconstitutional
- The Supreme Court's decision in *Facebook v. Duguid et al*. clarifying the definition of an "automatic telephone dialing system" or ATDS
- Standards for revocation of consent are in flux
  - *Medley v. Dish Network, LLC,* 958 F.3d 1063, 1070 (11th Cir. 2020) (holding that "common law contract principles do not allow unilateral revocation of consent when given as consideration in a bargained-for agreement")
- FCC Orders implementing STIR/SHAKEN
- TRACED Act revisions to the TCPA rules
- Reassigned number database

Barr v. American Association of Political Consultants Inc.

TCPA amended in 2015 to exempt calls relating to the collection of debts owed or guaranteed by the federal government.

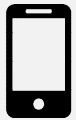
July 6, 2020

The Supreme Court issued its decision in *Barr v. American Association of Political Consultants Inc.*, invalidating the government-debt exception to the TCPA as unconstitutional, but leaving the rest of the ban on autodialed calls intact.

The Court concluded that through the government-debt exception, Congress has impermissibly favored debt collection speech over political and other speech in violation of the First Amendment.

District courts are split on the issue of whether *Barr* has any effect on the liability of calls other than government collection calls.

Barr v. American Association (cont'd)



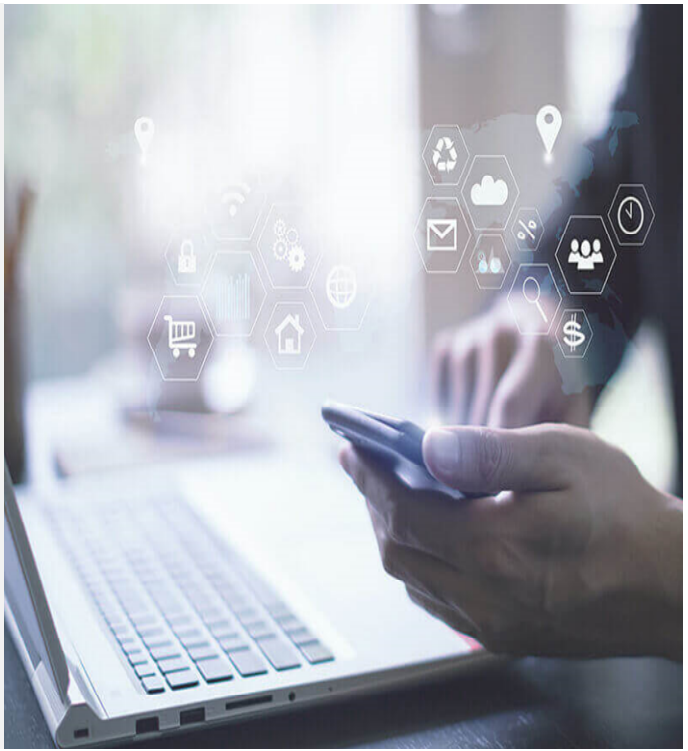
The TCPA remains the law of the land and is only strengthened by the decision.

In addition, the court appears to have been influenced in part by the perceived popularity of the TCPA, as Justice Kavanaugh notes that although Americans disagree about many things, they are "largely united in their disdain for robocalls."

Also, the *Barr* decision may also be used to challenge other aspects of the TCPA, such as exceptions for package delivery and certain types of healthcare messages. Given the court's conclusion that the exception for government debt collection was unconstitutional because it "single[d] out specific subject matter for deferential treatment," some may argue that the other exceptions are also problematic.

Definition of "Autodialer"

- To be liable under the TCPA, calls must be made with an "automatic telephone dialing system" or use a recorded message.
  - ATDS is defined as "equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers."
- The FCC's 2015 Omnibus Order addressed the definition of an ATDS and broadened the statutory definition of **"capacity"** to encompass "potential functionalities" and "future possibility."
- In *ACA Int'l. v. FCC*, 885 F.3d 687 (DC Cir. 2018), the DC Circuit held that the FCC's interpretation of ATDS in its 2015 Order leaves affected parties "in a significant fog of uncertainty about how to determine if a device is an ATDS so as to bring into play the restrictions on unconsented calls." The court did not provide any other guidance on the meaning of ATDS; instead, it found that any interpretation of "capacity" that includes smartphones is an unreasonable reading of the TCPA.



Supreme Court's Autodialer Decision

- *Facebook v. Duguid et al.* (April 1, 2021)-Long awaited clarification on the definition of an "automatic telephone dialing system," key term under the Telephone Consumer Protection Act (TCPA).
- TCPA requires prior express consent for any call or text sent with an ATDS.
- Statutory definition says an ATDS is equipment with the capacity "to store or produce telephone numbers to be called, using a **random or sequential number generator**," and to dial those numbers.
- Plaintiff argued that the phrase "using a random or sequential number generator" modified only "to produce"; Facebook said that it modified both "to produce" and "to store."
- The Court addressed a question facing thousands of companies: Is a system that merely stores and calls/texts customer numbers automatically an ATDS?

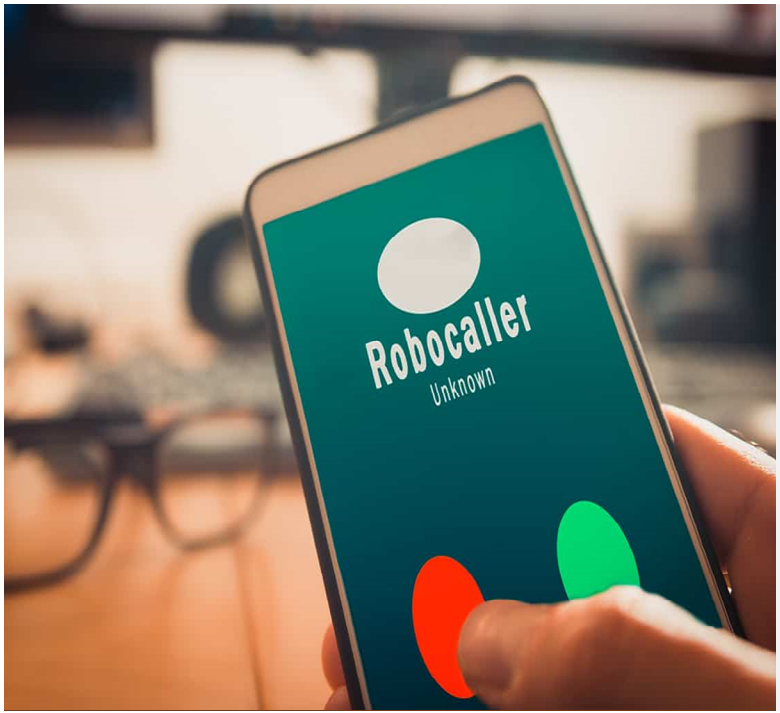
Supreme Court's Autodialer Decision (cont'd)

- Court held: Ruled 9-0 for Facebook.
  - Applying simple rules of grammar, an ATDS must have the capacity either to store a telephone number using a random or sequential number generator OR to produce a number using a random or sequential number generator.
  - Context confirms this reading since Congress's concern was that ATDS technology would dial emergency lines randomly or tie up all the sequentially numbered lines at a single entity.
  - The Supreme Court cannot reinterpret the statute to encompass new technology.
- Reduces risk for companies that text and call customers. **Systems that are just calling from a list are not an ATDS.**
- But not correct that you do not need consent:
  - Do Not Call Rules still apply
  - "Capacity" question
  - State law
  - Congressional action?

Revocation of Consent

- The TCPA does not elaborate on the processes by which consumers may validly revoke consent.
- The FCC's 2015 Order concluded that a "called party may revoke consent at any time and ***through any reasonable means***."
- In *ACA Int'l*, the DC Circuit upheld the FCC's 2015 ruling on revocation of consent, noting that establishing clearly-defined and simple opt-out methods is a way in which callers can protect themselves from liability: "callers will have every incentive to avoid TCPA liability by making available clearly-defined and easy-to-use opt-out methods. If recipients are afforded such options, any effort to sidestep the available methods in favor of idiosyncratic or imaginative revocation requests might well be seen as unreasonable."
  - In addition, the court stated that nothing in the FCC's 2015 order should be understood to speak to parties' ability to contractually agree upon revocation procedures.
- The DC Circuit offered two avenues that could be helpful to companies in avoiding TCPA litigation: (1) create clear and easy revocation methods and communicate those methods to consumers; and (2) negotiate the terms of revocation by contract.
- On May 1, 2020, the Eleventh Circuit held in a TCPA case that "common law contract principles do not allow unilateral revocation of consent when given as consideration in a bargained-for agreement." *See Medley v. Dish Network, LLC*, 958 F.3d 1063, 1070 (11th Cir. 2020).

FCC – Combat Against Robocalling



- **Multipronged Approach**
  - Attempting to clamp down on "spoofing"
  - Fantastic fines for violations of its Truth-in-Caller ID Rules
  - Extended Truth-in-Caller ID Rules to foreign calls and text messages
  - Selected a consortium of industry participants to lead traceback efforts
  - Adopted new rules allowing for call blocking in certain circumstances

STIR/SHAKEN

Secure Telephony Identity Revisited (STIR); Signature-based Handling of Asserted information using toKENs (SHAKEN)

Establishes industry standards and protocols for exchanging traffic allowing for verifying call information and easing tracing calls as they traverse different carriers' networks

Two components: (1) process of authenticating and verifying caller ID information; and (2) the certificate governance process that maintains trust in the caller ID authentication information transmitted along with a call

Relies on digital "certificates" to ensure trust

STIR/SHAKEN (cont'd)

- Governance Model
  1. Governance Authority
  2. Policy Administrator
  3. Certification Authorities
  4. Voice Service Providers
- TRACED Act directed the FCC to require by June 30, 2021, all voice service providers to implement STIR/SHAKEN

Telephone Robocall Abuse Criminal Enforcement Act

- "TRACED Act" signed into law Dec. 31, 2019
  - Expedites the FCC's Enforcement Authority
  - Increases statute of limitations for the FCC to pursue violators of ATDS and unsolicited fax rules from 1 to 4 years (Sec. 227(b))
  - Increases statute of limitations for violations of the Truth of Caller ID Act (Sec. 227(e))
  - Directs the FCC to adopt call authentication technologies to allow providers to verify that calls that touch its network are verified before terminated to consumers
  - Requires the FCC to evaluate other enforcement mechanisms
  - Several targeted provisions: reassigned number database, analysis of enabling of TCPA violations, "one-ring" scams

FCC Order Implementing TRACED Act

- Released by the FCC's Enforcement Bureau on May 1, 2020
  - Effectuates certain TRACED Act provisions without notice and comment
  - Violators of Section 227(b) are now subject to direct enforcement actions by the FCC
  - Provides the FCC with the ability to seek $10,000 per intentional unlawful robocall in addition to the FCC's preexisting forfeiture authority
  - Extends the statute of limitation period to four years for the FCC to pursue violators of Section 227(b) and (e)

FCC Recent Robocalling Developments

- Sixth Report and Order & FNPRM (Federal Register Publication May 5, 2023)
  - All providers must take "reasonable steps" to mitigate robocalling
  - Enhanced Robocall Mitigation Database Filings and Certifications
  - First Non-Gateway Intermediate Provider in Call Path Must Authenticate Calls
  - Non-Compliance Penalties Could Include Per-Call Forfeitures, Revocation of 214 Authority, and/or inability to obtain future authorizations
- Expanding Call Blocking Requirements (considered at May 18, 2023, Open Meeting)

Reassigned Numbers Database

Implementation

- On February 8, 2021, the FCC released a Public Notice announcing the compliance date for the final rule related to the Reassigned Numbers Database.
- Beginning April 15, 2021, and every 15th day of each month thereafter, service providers must report permanent disconnections of their subscribers.
- Small service providers (100,000 or fewer domestic retail lines) had six additional months (until October 15, 2021) to begin reporting to the Reassigned Numbers Database Administrator.

Reassigned Numbers Database (cont'd)

Safe Harbor

- Callers that make use of the database should not be subject to liability if the database reports that a number has not been reassigned and nevertheless it has been, and so a caller inadvertently calls a new consumer
- Caller must have reasonably relied upon the database when making a particular call
- Limited to the database established by the FCC Order
- Callers must demonstrate that they appropriately checked the most recent update of the database and the database reported "No" when given either the date they contacted that consumer or the date on which the caller could be confident that the consumer could still be reached at that number
- Callers bear the burden of proof and persuasion to show that they checked the database before making a call

COMPUTER FRAUD AND ABUSE ACT

Morgan Lewis

Computer Fraud and Abuse Act (CFAA)

- The CFAA subjects to criminal and civil liability anyone who "intentionally accesses a computer without authorization or exceeds authorized access." 18 U.S.C. § 1030(a)(2).
- The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).
- Clearly prohibits "hacking" where a third party is accessing a system for a malicious purpose, and it also extends to employees that exceed their authorized access.
- Split in circuits as to how broadly to interpret CFAA in the employment context. Specifically, does authorized access for an improper purpose violate the CFAA?

Van Buren v. United States (decided June 3, 2021)

Facts: Police officer (Van Buren) offered $5,000 to run a license plate check to determine whether the registered owner was an undercover police officer.

Charges: Among others, one criminal charge was for violation of the CFAA where prosecutors argued that Van Buren violated the CFAA in accessing the relevant database for an improper purposes.

Response: Van Buren argued that he did not exceed authorized access of the relevant computer system as he had authority to do so. The fact that he did it for an improper purpose is irrelevant for purposes of determining criminal liability under the CFAA.

Held: The Supreme Court agreed with Van Buren noting that to find otherwise would criminalize "every violation of a computer-use policy"

CFAA State of Play Post *Van Buren*

- CFAA inapplicable when users with legitimate access misuse such access and websites that make data publicly available cannot maintain a claim under the CFAA by attempting to restrict access to such data to a person.
- Other causes of action may still apply:
  - Common law claim of trespass
  - Copyright infringement
  - Breach of contract
  - Unjust enrichment
  - Conversion
  - Claims under state-specific statutes

CONGRESSIONAL ACTIVITY RELATED TO PRIVACY

Morgan Lewis

American Data Privacy and Protection Act

- Passed out of the Energy and Commerce Committee by a 53-2 vote last year
- Will require a reintroduction and restart to its legislative path in the House – March 1, 2023, House Innovation, Data and Commerce Subcommittee held a hearing to restart the process
- Largely preempt state laws but not all state laws
- 2023 sees six additional state privacy laws come into effect: Virginia, Colorado, Utah, Connecticut, California (CPRA) and Iowa

Data Privacy Act of 2023

- Introduced by Chair of the House Financial Services Committee Patrick McHenry
- Amend the Gramm-Leach-Bliley Act to provide consumers with more control over their PI
- Many existing state privacy laws include carevouts for entities governed by other federal laws like the GLBA
- Bill would preempt all relevant state laws in this field to the extent that carveouts do not apply or are not included in relevant state law
- Would require consent to use nonpublic information (NPI), requires notice of NPI collection not just disclosure, expands requirements for what must be included in privacy policies, directs state insurance authorities to issue regulations, expands definition of "financial institutions" to include "data aggregators", expands definition of NPI to include certain inferential information, etc.

Upholding Protections for Health and Online Location Data Privacy Act (UPHOLD)

- Introduced by Senators Amy Klobuchar (D-MN), Elizabeth Warren (D-MA), and Mazie Hirono (D-HI)
- Designed to prevent the use of personally identifiable health data for commercial advertising
- Would place additional disclosure restrictions on companies using personal health information without user consent and bans the sale of precise location data

SECURITIES AND EXCHANGE COMMISSION

Morgan Lewis

SEC Proposes Three Cybersecurity Rules

1. Would require SEC-registered brokers, dealers, investment companies, and investment authorities to adopt written policies and procedures to address unauthorized access to, or use of, customer information
2. Would require certain entities (e.g., broker-dealers, clearing agencies, and national securities associations) to address cybersecurity risks through policies and procedures, notify and report cybersecurity incidents to the SEC, and publicly disclose such incidents to improve transparency
3. Would expand the scope of entities subject to regulations systems compliance and integrity, bringing within its scope registered security-based swap data repositories, exempted clearing agencies, and certain large broker-dealers

RONALD W. DEL SESTO, JR.

Ron Del Sesto
Washington, DC
+1.202.373.6023
ronald.delsesto@morganlewis.com

Ron Del Sesto represents technology companies on a broad range of issues including corporate, financial, regulatory, and cybersecurity. Ron also advises financial institutions, private equity firms and venture capital funds with respect to investments in the telecommunications, media, and technology (TMT) sectors. Ron also counsels clients on privacy issues that implicate a myriad of federal statutes and rules, including the FCC's Customer Proprietary Network Information (CPNI) rules; retention marketing and "winback" rules; the Telephone Consumer Protection Act (TCPA); the FTC's Identity Theft or Red Flag Rules; the Telemarketing Sales Rules; and the CAN SPAM Act. He advises clients with respect to the use of location-based data by mobile applications, assists clients in implementing "best practices" when handling personally identifiable information, and is familiar with the self-regulatory industry practices established by various trade associations as well as FTC rulings and other reports and analyses released by the FCC, the FTC, and state attorneys general that provide guidance to the industry.

GREGORY T. PARKS

Gregory T. Parks
Philadelphia
+1.215.963.5170
gregory.parks@morganlewis.com

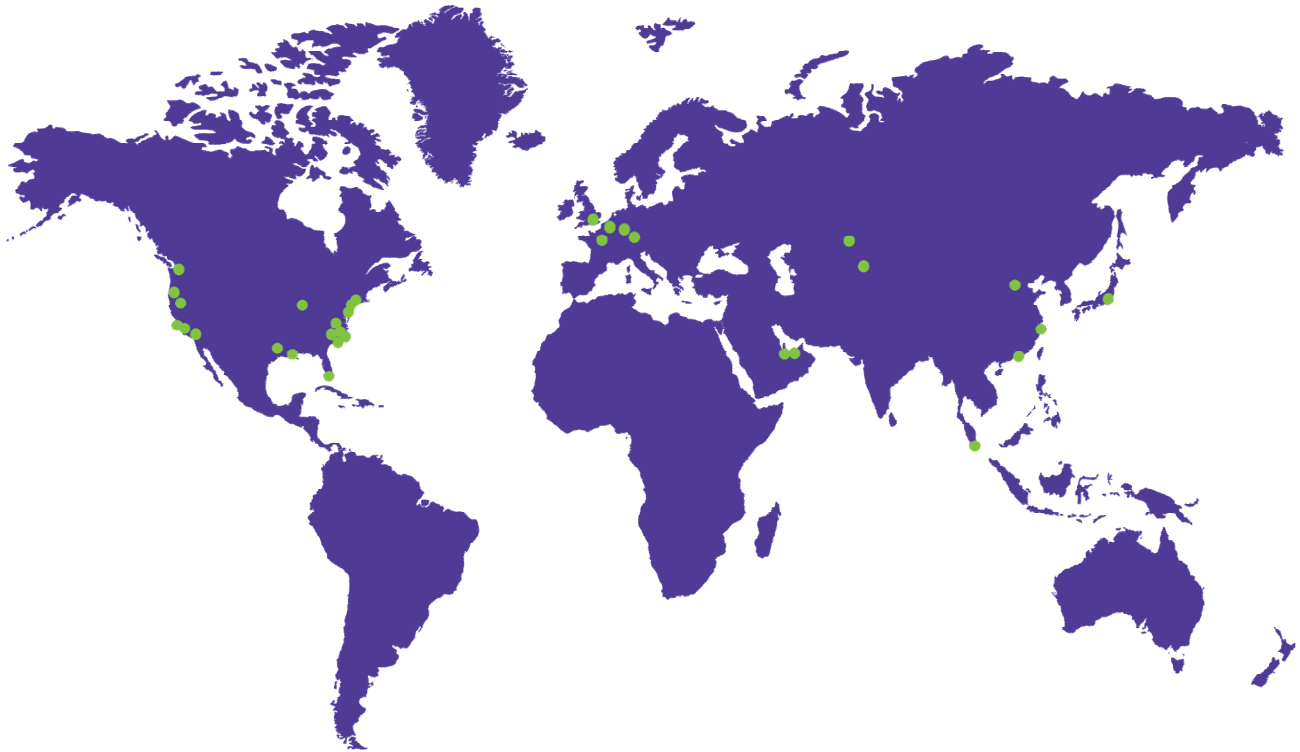
Co-leader of the firm's privacy and cybersecurity practice and retail & ecommerce sector, Gregory T. Parks counsels and defends consumer-facing clients in matters related to privacy and cybersecurity, class actions, Attorney General investigations and enforcement actions, the California Consumer Privacy Act, consumer protection laws, loyalty and gift card programs, retail operations, payment mechanisms, product liability, retail waste, shoplifting prevention, compliance, antitrust, commercial disputes, and a wide variety of other matters for retail, ecommerce, and other consumer-facing companies. Greg also handles data security incident response crisis management and any resulting litigation, and manages all phases of litigation, trial, and appeal work arising from these and other areas.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Astana
Beijing
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong
Houston
London
Los Angeles
Miami
Munich
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU