Morgan Lewis

TECHNOLOGY MARATHON

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

Greg Parks, Ron Del Sesto, Terese Schireson, Trina Kwon

Wednesday, May 1, 2024

Presenters

Gregory T. Parks

Ronald W. Del Sesto, Jr.

Terese M. Schireson

Trina Kwon

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 7/1/2027

- Confirmed by Senate for second term in September 2023
- Former prosecutor with experience in FCC Enforcement Bureau

Brendan Carr (R), term expires 6/30/2028

- Former advisor to FCC member Ajit Pai, briefly served as General Counsel of FCC
- Confirmed by Senate for second term in September 2023

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

- Former senior advisor at NTIA
- Confirmed by Senate on 12/8/2020

Anna Gomez (D), term expires 6/30/2026

- Former deputy assistant secretary of NTIA
- Confirmed by Senate in September 2023

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- In 2018, under Republican leadership, the FCC repealed the 2015 order, classifying broadband as a Title I information service resulting in eliminating the FCC's authority to impose Net Neutrality rules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
- On April 25, 2024, Chair Rosenworcel and the majority Democrat FCC voted to restore Net Neutrality, essentially reinstating provisions of the 2015 order, reclassifying broadband service as telecommunications service, and reestablishing greater authority over broadband service providers

Net Neutrality (cont'd)

- The new Net Neutrality order seeks to bring back 2015 "bright-line" rules and moves to classify internet service providers as Title II carriers (subject to most 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 or affiliated 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 does not propose 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, including universal service contributions

There are some notable distinctions from the 2015 order

- Contemplates licensing framework for ISPs under Section 214 of Communications Act, potentially resulting in increased Team Telecom review of ISP transactions
- No forbearance from Title III licensing authorities
- Highlights national security and cybersecurity justifications

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
  - Penalties have been issued for defaults under the Rural Digital Opportunity Fund

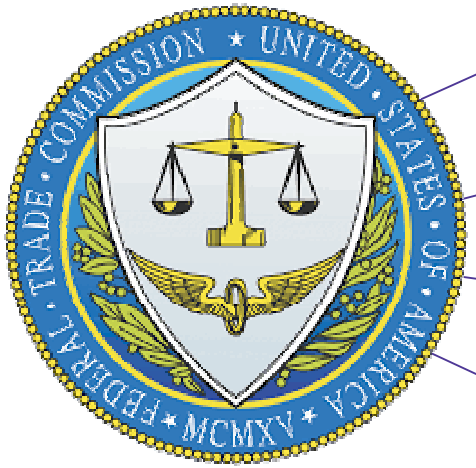
Section 230

- Section 230 of the 1996 Communications Decency Act shields online publishers from liability for content generated by users
- Calls for reform of Section 230 have increased; Biden appears to have supported repeal of Section 230 (wholesale elimination is not, however, expected)
- 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 that the FCC has the authority to interpret Section 230
- The FCC will most likely defer to Congress
- On April 11, 2024, House Subcommittee on Communications and Technology held hearing on reforming Section 230

THE FEDERAL TRADE COMMISSION

Morgan Lewis

Federal Trade Commission (FTC)

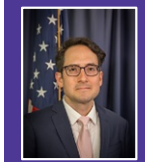


- Led by five Commissioners nominated by the President and confirmed by the Senate
- Each serves a seven-year term
- No more than three Commissioners can be from the same political party
- President selects one Commissioner to act as Chair

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

Melissa Holyoak (R) – Commissioner and sworn in March 25, 2024

Andrew Ferguson (R) – Commissioner and sworn in April 2, 2024

FTC Agenda Under the Biden Administration

- Internet Services and Telecom
  - Illegal telemarketing, data security practices, online subscriptions or purchases, deceptive practices regarding user reviews and COPPA violations
- Financial Services
  - Debt collection, debt relief and credit repair, hidden loan application fees, payday loan overcharges and deceptive marketing of investment-related services
- Healthcare
  - Deceptive marketing and health data privacy; update federal FTC Health Breach Notification Rule
- Retail
  - Labeling or marketing of products, deceptive or fraudulent endorsements, consumers' right to repair and data privacy practices
- Other priorities: AI, junk fees, consumer endorsements

FTC Agenda Under the Biden Administration (cont'd)

- 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
  - While awaiting Congressional fix, FTC is employing tools like trade regulations allowing for civil penalties (e.g., TSR, ROSCA, COPPA, Made in USA Labeling Rule)

FTC Agenda Under the Biden Administration (cont'd)

- Consumer Data Privacy Protection Enforcement
  - *In the Matter of Ring, LLC* – Ring failed to implement basic security protections, enabling hackers to take control of consumers' accounts, cameras, and videos
    - Imposed $5.8 million penalty and imposed injunctive measures, including mandatory deletion of affected data
  - *In the Matter of X-Mode Social, Inc.* – X-Mode sold precise location data
    - Imposed injunctive measures, including prohibition on disclosure or sale of sensitive location data

FTC Agenda Under the Biden Administration (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
  - Edmodo, LLC (Aug. 2023) – Education technology provider
    - FTC alleged violation of COPPA for collecting children PI data without parent's consent and using that data for advertising, and for unlawfully outsourcing COPPA compliance responsibilities
    - $6 million settlement order and other injunctive relief
  - FTC NPRM proposing amendments to COPPA (published December 20, 2023), which would:
    - Enhance parental control over children's data for disclosures to third parties
    - Provide additional guidance to operators on implementation measures for data security, including data deletion and retention
    - Expand scope of PI to include biometric information

FTC Agenda Under the Biden Administration (cont'd)

- Focusing on Effective Remedies
  - 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
- Released an Advanced Notice or Proposed Rulemaking on Aug. 11, 2022, considering commercial surveillance and data security practices
  - Comment period ended Nov. 21, 2022
  - Included 95 questions covering a broad rane of topics including harms caused by commercial surveillance, data security practices, AI-related issues and regulatory enforcement measures
  - Controversial Magnuson-Moss rulemaking process

FTC's Reboot of health Breach Notification Rule -- Background

- "HIPAA gets all the press"
- HIPAA "loophole" because it only applies to covered entities – health care providers or those involved in obtaining HCP insurance reimbursement.
- FTC initial promulgated rule in 2009 to cover vendors of "personal health records" (PHR)
- Key portion is "managed, shared, and controlled by or primarily for the individual."
- But perceived loopholes in the loophole fix

FTC's Reboot of health Breach Notification Rule – What's New?

- Applies to apps (clarification)
- Covers unauthorized disclosures (oops)
- *Capacity* to draw from multiple sources
- Notify FTC and >500 consumers at same time, within 60 days of discovery
- New focus *primarily* on electronic notice (away from first class mail)
- Must disclose the identify of any third parties that acquired compromised information

ROBOCALLING/TEXTING

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
- FCC Orders restricting AI-generated voices in robocalls, closing lead generator loophole, and clarifying revocation of consent

STIR/SHAKEN Expansion

- In March 2023, FCC expanded some robocalling mitigation obligations to all providers that carry voice traffic, including intermediate providers, providers that have already implemented STIR/SHAKEN, and other providers previously not subject to compliance obligations
- Staggered deadlines to come into compliance:
  - Must have implemented new obligations – i.e., taking "reasonable steps" to mitigate robocalls and instituting comprehensive mitigation plans – by August 21, 2023
    - Downstream providers must block traffic from intermediate providers not in the Robocalling Mitigation Database
  - By end of 2023, all non-gateway intermediate providers were required to authenticate unauthenticated SIP calls from an originating provider
  - By February 26, 2024, all carriers that offer voice services or carry voice traffic had to submit new or updated Robocall Mitigation Database (RMD) certifications and Robocall Mitigation Plans

AI-Generated Robocalls

- On February 8, 2024, FCC released declaratory ruling prohibiting AI-generated robocalls
- FCC found that calls using AI technologies resembling human voices, e.g., "voice cloning," falls within TCPA's prohibition on artificial or prerecorded voice messages
- Callers must obtain prior express consent from called party before making calls using AI-generated content, absent emergency purpose or exemption provided under TCPA

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).

Revocation of Consent (cont'd)

- On February 16, 2024, FCC issued Order amending rules and offering further guidance on revocation of consent:
  - Consumers may revoke prior express consent by using any reasonable method and cannot be restricted to designated exclusive means by callers/senders
  - Reasonable methods include:
    - Using automated, interactive voice or key press-activated opt-out mechanism;
    - Using responses of words like "stop," "cancel," "unsubscribe," etc., in reply to text message; and
    - Submitting opt-out requests to website or telephone number provided by caller.
  - When text initiator does not allow reply texts, must provide clear disclosure of inability to reply and reasonable alternatives to revoke consent
  - If consumer uses method not listed in the regulation, rebuttable presumption of revocation when the consumer produces evidence that request has been made
  - Request to revoke consent must be honored within reasonable time not to exceed ten business days from receipt

FCC'S CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

Morgan Lewis

CPNI Rules - Background

- 1998 – Initial Adoption of CPNI Rules
  - CPNI defined as information about customers' telecommunications services, including call detail records and location data
  - Subject to limited exceptions, carriers prohibited from disclosing CPNI without consent
  - Opt-in consent required for use of CPNI for marketing purposes
- 2007 – FCC Amends Rules
  - Scope expanded to include providers of interconnected VoIP services
  - Imposed new data safeguards and authentication requirements on carriers
  - Opt-in consent expanded, disclosures of CPNI to (1) joint venture partners; (2) independent contractors
- 2013 – Key Revisions to CPNI rules
  - Required annual notification to consumers of their rights with respect to CPNI
  - Imposed new data breach notification requirements on carriers

CPNI Rules – 2023 Order

- December 2023 Order
  - Expands CPNI definition to include customers' personally identifiable information (PII)
  - Revised definition of breach to include any inadvertent access, use or disclosure of customer PII data
  - Adopts a "harm" based trigger for notifying customers of certain CPNI breaches
  - Requires carriers to notify the FCC, law enforcement, and customers of any breaches without undue delay and within 30 days
  - Imposes minimum notice requirements
  - Adopts new authentication requirements for account changes like SIM swaps or port-outs
  - Requires the use of multi-factor authentication methods to verify customers before making changes
  - Mandates that carriers notify customers of any failed authentication attempts on their accounts

RECENT CPNI ENFORCEMENT ACTION

- Apr. 29, 2024 – FCC Releases Orders in connection with Feb. 28, 2020, NALs
  - 3-2 vote with Commissioners Carr and Simington dissenting
  - Major wireless carriers allegedly disclosed customers' location information to 3rd parties without consent
  - Four carriers collectively fined close to $200 million for violating the FCC's CPNI rules
  - Opt-in consent required prior to disclosing CPNI to 3rd parties pursuant to *2007 CPNI Order*
  - All customers' location information constitutes CPNI not just in connection with a call
  - Location information made available only by virtue of the carrier customer relationship
  - Carriers held responsible for unauthorized access to CPNI by third parties
  - Carriers intend to appeal

CONGRESSIONAL ACTIVITY RELATED TO PRIVACY

Morgan Lewis

American Privacy Rights Act

- On April 7, 2024, Sen. Maria Cantwell (D), Chair of the Commerce Committee, and Rep. Cathy McMorris Rodgers (R), Chair of the Energy and Commerce Committee, unveiled the draft privacy legislation
- On April 17, 2024, the House Energy and Commerce Committee held a hearing to discuss the discussion draft of the American Privacy Rights Act ("APRA")
- Widely held to be the best chance at passing national, comprehensive privacy legislation Congress has considered yet

American Privacy Rights Act

- Applicability:
  - Commercial enterprises
  - Nonprofit organizations
  - Common carriers
  - *Small businesses generally exempt if: (a) <$40 million in revenue, (b) only has data about less than 200k consumers, (c) acting as "covered entity" (i.e., not service provider), and (d) does not sell data to a third party.
- Key Definitions:
  - "Covered data" – information that "identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals"
    - Exemptions: Deidentified data, information in libraries, and inferences from publicly available information, as long as not combined with covered data and do not reveal sensitive information
  - "Individual" – US residents

American Privacy Rights Act

- Key Obligations:
  - Data minimization, i.e., presumption of prohibition on processing of personal data, unless necessary, proportionate, and limited for listed permitted purposes
  - Transparency of privacy policies
  - Consumer rights to covered data
  - Opt-out rights and centralized opt-out mechanisms
  - Prohibition on interference with consumer rights, including dark patterns
  - Prohibition on denial of service and waiver of rights
  - Data security practices
  - Executive responsibility
  - Due diligence of service providers and third parties
  - Civil rights
  - Opt-out rights to consequential decisions using covered algorithms

American Privacy Rights Act

- Other Key Takeaways:
  - Private right of action
    - Individuals may sue under many (but not all) operative provisions, including violations of opt-in consents for sensitive data transfers; use of dark patterns that interfere with notice, consent, or choice; processing covered data that unlawfully discriminates, etc.
    - Limitations on arbitration agreements between companies and individuals – i.e., such pre-dispute arbitration agreements would be invalid for minors and "substantial privacy harm"
  - Preemption of state consumer privacy bills
    - However, (a) would empower same state enforcers to enforce APRA and (b) carves out from preemption certain state laws, including employee privacy, student privacy, data breaches, civil rights, etc.

Consumer Privacy

- Banning Surveillance Advertising Act of 2022 – Prohibits targeted advertising under certain circumstances
- Online Privacy Act of 2021 –
  - Opt-in consent required for disclosure and sale of PI
  - Requires data minimization and reasonable cybersecurity practices
  - Right to access, correct, delete, and to port data
  - Would create a federal digital privacy agency
- Informing Consumers about Smart Devices Act – Imposes disclosure obligations on manufacturers of IoT devices that include cameras and microphones

FTC-Related Legislation

- Algorithmic Accountability Act of 2023 – Mandates that the FTC require impact assessments of automated decision systems. Note that the FTC included this issue for consideration in its rulemaking.
  - Bicameral legislation was introduced in September 2023
- Protecting Consumers from Deceptive AI Act – Requires any provider of generative AI applications to make disclosures to users that any audio or visual content has been created or modified using such applications. Would authorize FTC enforcement authority for any violations of disclosure obligation.
  - Legislation introduced in House on March 21, 2024

NEW SEC CYBERSECURITY RULES

Morgan Lewis

SEC Rules

- Adds a new Item 1.05 to Form 8-K requiring disclosure of material cybersecurity incidents; and
- Through revisions to Form 10-K and the addition of a new Item 106 to Regulation S-K, requires periodic disclosures regarding cybersecurity matters, namely
  - the processes employed by a company to assess, identify, and manage cybersecurity risks;
  - whether any cybersecurity risks have materially affected or are reasonably likely to materially affect a company's business strategy, results of operations, or financial condition;
  - management's role in assessing and managing material risks from cybersecurity threats; and
  - the board of directors' oversight of cybersecurity risk.

Section 1.05c

- Accordingly, and unlike the Proposed Rule's suggestion, the new Item 1.05 of Form 8-K mandated by the Final Rule does not affirmatively require disclosure of technical information about an incident's remediation status (e.g., whether it is ongoing or whether data were compromised) or "potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident," though companies should take such factors into consideration in their materiality analysis.
- Instead, the more streamlined Final Rule requires that, upon determining that a cybersecurity incident is material, a company more broadly describe:
  - the material aspects of the nature, scope, and timing of the incident, and
  - the material impact or reasonably likely material impact on the company, including its financial condition and results of operations.
- Narrow exception if US Attorney General determines disclosure poses a substantial risk to national security or public safety

Materiality Determination

- The Final Rule provides and references nonexhaustive examples of factors the SEC would expect companies to consider in making materiality assessments, many of which may be difficult to quantify:
  - Reputational damage (which is mentioned several times in the Final Rule);
  - Data theft;
  - Asset, intellectual property, or business value loss;
  - Harm to customer or vendor relationships;
  - Competitive harm; and
  - The possibility of litigation or regulatory investigation or actions.
- Reasonable investor standard

Annual 10-k Disclosures; a company must:

- Describe its processes, if any, for the identification and management of risks from cybersecurity threats, including
  - whether such cybersecurity processes have been integrated into the company's overall risk management system or processes;
  - whether the company engages third-party assessors, consultants, or auditors in connection with any such processes; and
  - whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service providers; and
- Provide disclosure about the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing material cybersecurity risk and implementing the company's cybersecurity policies, procedures, and strategies, including
  - whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members (in such detail as necessary to fully describe the nature of the expertise);
  - the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
  - whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

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.

TERESE M. SCHIRESON

Terese M. Schireson
Philadelphia
+1.215.963.4830
terese.schireson@morganlewis.com

Terese M. Schireson represents clients in diverse areas, including privacy and cybersecurity, class action litigation, and complex commercial disputes, in state and federal courts across the country. She primarily counsels and defends clients in matters relating to compliance with new consumer privacy laws, data security incident response, and any related litigation or government investigations. Terese also defends companies in litigation involving breach of contract, unfair competition, fraud, and consumer protection claims and advises consumer-facing clients on legal, regulatory, and operational matters. She serves clients across diverse industries, including the retail, energy, technology, and healthcare sectors. Terese is a member of the firm's global privacy and cybersecurity practice as well as its Class Action Working Group.

TRINA KWON

Trina Kwon
Washington, DC
+1.202.739.5475
trina.kwon@morganlewis.com

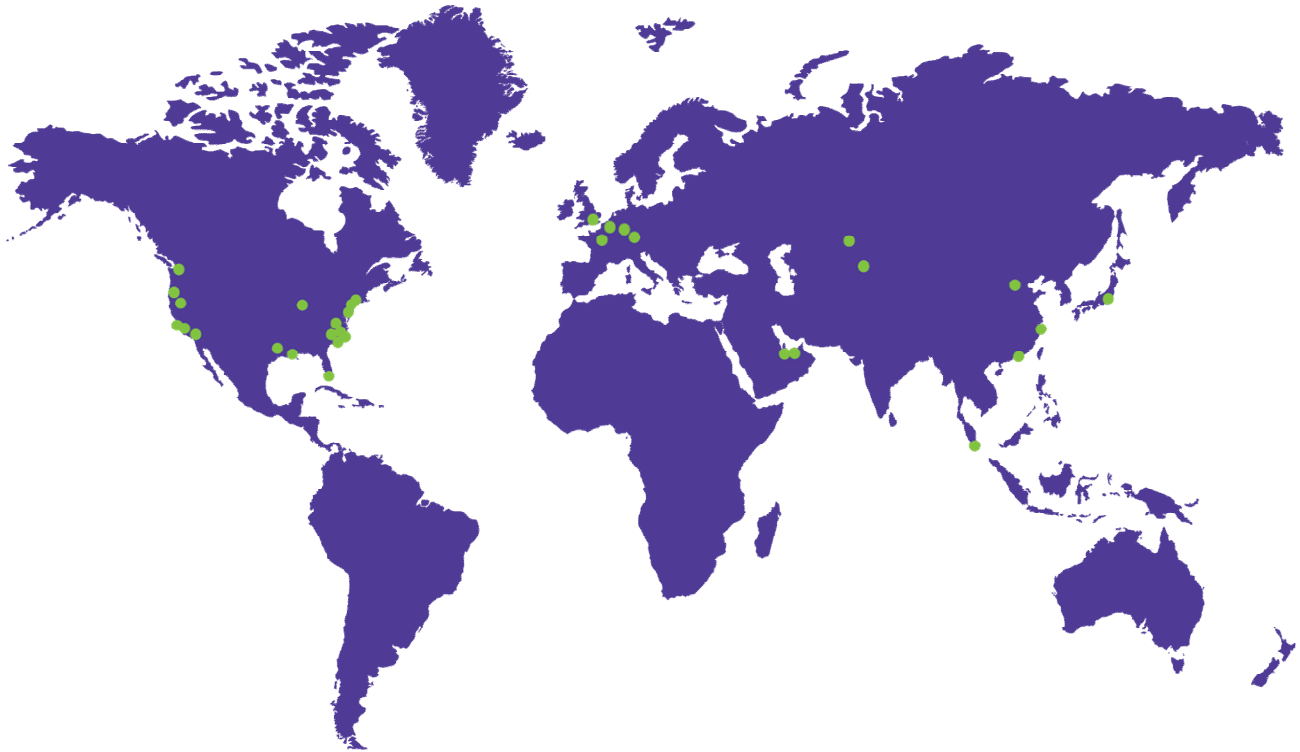
Trina Kwon represents domestic and international clients in the technology and communications industry in various transactional, regulatory, and litigation matters. She assists clients with structuring and negotiating technology agreements, including licensing and networking infrastructure contracts such as submarine cable joint build and supply agreements, master services agreements, telecommunications services procurement, and cloud computing contracts. Trina also advises financial institutions, private equity firms, and venture capital funds on investments in the telecommunications, media, and technology (TMT) sectors and other financial arrangements. She also assists clients with respect to federal privacy issues.

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