



Morgan Lewis

PRIVACY AND DATA SECURITY TRENDS AT THE FTC, FCC AND STATE ATTORNEYS GENERAL

Ronald Del Sesto, Jr. and Gregory Parks

May 24, 2018

Roadmap



- Federal Communications Commission
- FCC – Privacy and Data Security
- Network Neutrality
- FTC/FCC Jurisdictional Scope
- New Slate of Federal Trade Commission Commissioners
- Tangible Harm and IoT
- The Telephone Consumer Protection Act
- State Update
- Congressional Activities

Morgan Lewis

SECTION 01

**THE FEDERAL COMMUNICATIONS
COMMISSION**

Federal Communications Commission



- Chairman Ajit Pai (R)
- Commissioner Michael O’Rielly (R)
- Commissioner Brendan Carr (R)
- Commissioner Clyburn (D)
- Commissioner Rosenworcel (D)

Chairman Pai's Agenda

- Commissioner Pai:
 - “We need to fire up the weed whacker and remove those rules that are holding back investment, innovation and job creation”
- Chairman Pai has implemented process reforms
 - He has made the text of draft orders that will be considered at FCC Open Meetings available prior to the vote
 - He has circulated items that will be considered at an FCC Open Meeting to other commissioner offices prior to the Chairman's office making public statements concerning such items

Chairman Pai's Agenda



- Rollback Net Neutrality
- Undo Broadband Privacy and Data Security Order
 - Congress beat Chairman Pai to the punch through the Congressional Review Act
- Focus on broadband deployment

FCC – Privacy and Data Security



- Spectrum Frontiers Order – July 2016
 - Section devoted to cybersecurity
- Fifth Generation (5G) Wireless Network and Device Security Notice of Inquiry – December 2016
 - Literally released as former Chairman Tom Wheeler was ending his term
 - Sought comment on privacy and data security issues

FCC – Privacy and Data Security



- Restoring internet freedom (also referred to as Network Neutrality) – January 2018
 - Reclassification of Broadband Internet Access Services
 - Recent 9th Circuit decision in *FTC v. AT&T Mobility*
- Communications, Security, Reliability and Interoperability Council (CSRIC)
- Alleged Nationalization of the 5G networks
- Protecting against national security threats to communications supply chain through FCC programs

Network Neutrality



- December 2017 – FCC votes to repeal network neutrality rules effective June 11, 2018
 - Re-classify broadband service as a Title I information service
 - Mobile broadband service classification revised to private mobile service standard
 - Proposes that the FTC would regulate broadband ISP’s privacy practices
 - Seeks comment on conducting a cost-benefit analysis
 - Proposes to conduct a “regulatory analysis”
 - Costs of maintaining Title II should be estimated as those costs of *ex ante* FCC regulation relative to FTC *ex post* regulation
 - Former Acting Chair Ohlhausen expresses support for FCC’s proposed approach

Network Neutrality



- States pass or consider legislation that would restore the FCC's 2015 Open Internet Order
- May 2018 – ITIF proposes legislative solution is needed and should:
 - a) Prohibit blocking or throttling
 - b) Allow paid prioritization is important (points to IoT offerings that require time-critical applications like self-driving cars and remote surgery)
 - c) Preserve equality among less critical applications
 - d) Restore FCC jurisdiction over broadband services
- May 16, 2018 – Senate Democrats force a vote under CRA to repeal FCC December 2017 network neutrality order

SECTION 02

FTC/FCC JURISDICTIONAL SCOPE

FTC v. AT&T Mobility, LLC

- FTC alleged that AT&T committed an “unfair and deceptive” act in violation of Section 5 of the FTC Act by “throttling” data for “unlimited” data users.
- AT&T moved to dismiss, citing exemption for “common carriers”
- District Court denies motion, finding that “common carrier” exception only applies to activities as a common carrier.
- 9th Circuit reverses – ruling that “common carrier” exception applies to anything a common carrier may do.
- May 2017 – 9th Circuit grants FTC’s request for en banc review.

FTC v. AT&T Mobility, LLC

- February, 2018 – en banc court finds that the FTC has jurisdiction over non-common carrier activities of common carriers.
- Significant Decision:
 1. FTC can enforce antitrust and consumer protection law against common carriers for certain offerings
 2. The FCC and the FTC have a role in regulating common carriers depending on the offering
 3. Important decision with respect to the ongoing network neutrality debate

SECTION 03

THE FEDERAL TRADE COMMISSION

New Slate of FTC Commissioners



- Joseph J. Simons (R) – Chairman
- Maureen Ohlhausen (R) – Commissioner
- Noah Joshua Phillips (R) – Commissioner
- Rohit Chopra (D) – Commissioner
- Rebecca Kelly Slaughter (D) – Commissioner
- Christine Wilson (R) (not yet seated)

New Slate of FTC Commissioners

- Joseph J. Simons (R) – Chairman
 - Comes from private practice
 - Director of FTC Bureau of Competition under George W. Bush
 - Not a deep record on consumer protection issues
 - Confirmation hearing: Cybersecurity is critical issue and FTC must protect consumers but must do so “without unduly burdening [companies] or interfering with the ability of firms, especially small firms and new entrants to use data to enhance competition.”
- Maureen Ohlhausen (R) – Commissioner (former Acting Chair)
 - Repeatedly expressed desire that the FTC approach “intervention decisions with a philosophy of regulatory humility . . . [such that] government actors must heed the limits of their knowledge, consider the repercussions of their actions, and be mindful of the private and social costs that government actions inflict.”
- Noah Joshua Phillips (R) – Commissioner
 - Chief Counsel to Sen. John Cornyn (R-TX) on the Senate Judiciary Committee
 - Advised on privacy and antitrust issues

New Slate of FTC Commissioners



- Rohit Chopra (D) – Commissioner
 - Holds an MBA and served as a senior fellow at the Consumer Federation of America
 - Senior leadership at the Department of Education
 - Assistant Director of the Consumer Financial Protection Bureau and agency’s first student loan ombudsman
- Rebecca Kelly Slaughter (D) – Commissioner
 - Chief Counsel to Sen. Minority Leader Chuck Schumer (D-NY)
 - Worked in private practice previously
- Christine Wilson (R) (not yet seated)
 - Senior Vice President at Delta Air Lines
 - Responsible for regulatory and international matters
 - Chief of Staff under FTC Chairman Tim Muris

FTC Under Ohlhausen

- January 2016: FTC Releases Staff Report on Big Data
 - Then Commissioner Ohlhausen issued a separate statement
 - Highlights that businesses have strong incentives to compile accurate information about consumers, and market forces act to correct inaccuracies
 - Hypothetical harms must be tested by economic reasoning and empirical evidence
- **Opt-in consent**: For unexpected collection or use of consumers' sensitive data such as Social Security numbers, financial information, certain geolocation data and information about children.
- **Opt-in vs. Opt-out**: Regulations should maximize benefits while minimizing the costs. Opt-in or opt-out defaults should match typical consumer preferences such that costs (in the form of time and decision making) should only be imposed on consumers when it really matters. For sensitive information, this means opt-in; for non-sensitive information, opt-out.
- **Do No Harm**: "If a regulation imposes defaults that do not match consumer preferences, it imposes costs on consumers without improving consumer outcomes. The burdens imposed by a broad opt-in requirement may also have negative effects on innovation and growth."

FTC – Tangible Harm

- Privacy and Data Security – FTC relies on Section 5 of the FTC Act which prohibits unfair and deceptive practices.
 - *FTC v. D-Link Corp.*
 - *LabMD Inc. v FTC*
 - December 2017 Information Injury Workshop
 - January 2018 – Settlement with VTech Electronics
 - PayPal Settlement

FTC – Internet of Things



- IoT refers to things “such as devices or sensors . . . that connect, communicate or transmit information with or between each other through the internet.”
Internet of Things, FTC Staff Report, January 2015
- FTC’s jurisdiction limited to devices that are sold to or used by consumers
- Report, Mobile Security Updates – Understanding the Issues (Feb. 2018)
 - Focused on mobile handset manufacturers
 - Guidance not law, but will serve to inform the FTC when evaluating privacy and data security practices of company under Section 5 of the FTC Act
 - Broader guidance for IoT devices

SECTION 4

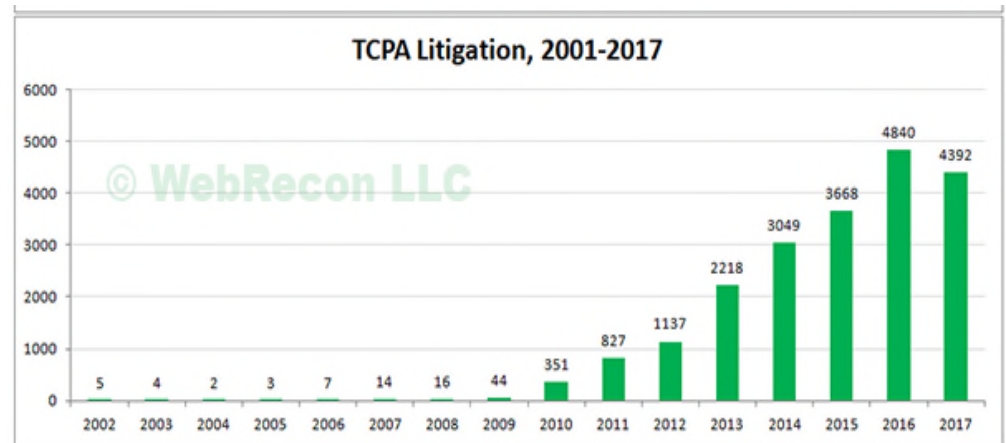
THE TCPA

Telephone Consumer Protection Act (TCPA)

- Passed in 1991 to regulate robocalling and unsolicited faxes
- Expanded to include text messaging in 2003
- FCC has primary jurisdiction to interpret the TCPA
- FCC, FTC, and state AGs can enforce the act, and it includes a private right of action
- \$500 per violation; trebled if willful

Telephone Consumer Protection Act (TCPA)

- ATDS is defined as equipment with the **capacity**: to store or produce telephone numbers to be called, using a random or sequential number generator
- Prohibits use of an ATDS to dial any telephone number assigned to a wireless service provider, or any service where called party is charged for the call
- Unless caller has the **prior express consent** of the called party or for emergency purposes



Telephone Consumer Protection Act (TCPA)

- FCC July 2015 Declaratory Ruling and Order
 - Broadened definition of “capacity”
 - Complicated revocation of consent for businesses
 - Liability for reassigned numbers
- Former Commissioner and now Chairman Pai’s and Commissioner O’Rielly’s positions regarding the TCPA
- *ACA International v. FCC*, affirming part and vacating in part *2015 FCC Order*
 - ATDS definition
 - Reassigned numbers
 - Revocation of consent
 - Scope of healthcare exemption

Morgan Lewis

Telephone Consumer Protection Act (TCPA)

- Impact of DC Circuit Decision
 - *Marshall v. CBE Grp., Inc.* (D. Nev. Mar. 30, 2018)
 - *Reyes v. Bca Fin. Servs.* (S.D. Fl. May 14, 2018)
 - *Herrick v. GoDaddy.com LLC* (D. Az. May 14, 2018)
- FCC Consumer and Governmental Affairs Bureau Public Notice May 14, 2018
- Comments Due June 13, 2018; Reply Comments Due June 28, 2018
 1. What constitutes an ATDS? (a) capacity; (b) functions; (c) random or sequential number generator of an ATDS; and (d) making a call using an ATDS
 2. Reassigned numbers and meaning of “called party”
 3. Revocation of consent
 4. Certain rules relating to calls placed when collecting debts to federal government

Bais Yaakov of Spring Valley, et al. v. FCC

- **Procedural Background**

- **2006:** FCC adopts an Order requiring fax senders to include an opt-out notice on *solicited* fax advertisements.
- **2010:** A party files a Petition for Declaratory Ruling of the FCC rule requiring opt-out notices for solicited fax advertisements.
- **2012:** CGA Bureau rejects petition on procedural grounds: (i) no basis for relief; and (ii) impermissible collateral challenge of the rule. Notes that it would reject the Petition on substantive grounds, too. Subsequently, same party files a Petition for Review.
- **Oct., 2014:** Commission affirms Bureau's finding and denies relief.
 - Pai/O'Rielly Dissent: statute is clear in its application exclusively to *unsolicited* fax advertisements; FCC interject uncertainty in its interpretation and then relies on such uncertainty to fill in gaps; point out procedural defects with the initial adoption of the rule.

Bais Yaakov of Spring Valley, et al. v. FCC

- **Opinion (2-1 Decision by DC Circuit)**
 - Relevant statutory provisions clearly distinguish between unsolicited and solicited fax advertisements.
 - The act does neither provides for nor grants the FCC with the authority to require opt-out notices on solicited fax advertisements.
 - Majority highlights that both the FCC and the dissent share the position that provided Congress has not prohibited an agency to engage in an action, it may do so. Majority disagrees, instead, Congress must authorize agency action.
 - Vacates the FCC's 2006 Solicited Fax Rule.

***Spokeo, Inc. v. Robins* (2016)**

- Cert denied January 22, 2018, on appeal of second Ninth Circuit ruling.
- “Article III standing requires concrete injury even in the context of statutory violation.”
- A plaintiff cannot “allege bare procedural violation, divorced from any concrete harm, and satisfy the injury in fact requirement of Article III.”
- Congress “cannot erase Article III’s standing requirements by statutorily granting the right to sue a plaintiff who would not otherwise have standing.”
- Impact on the TCPA:
 - Still evolving but appears effective with respect to *de minimis* communications by the defendant, e.g., receipt of a single or a few calls or text messages by the plaintiff.
 - Winning on standing does not necessarily mean no further liability.

SECTION 5

STATE UPDATE

State Data Breach Laws



- **Alabama** and **South Dakota** Enact Data Breach Notification Laws
- South Dakota Data Breach Notification Law
 - Mar. 21, 2018, signed into law
 - Similar to many other states' laws with respect to type of information that must be breached
 - Requires that a breach must be likely to result in harm to affected resident to trigger notification obligations
 - Even in absence of risk of harm, notice still must be provided to state attorney general
 - AG can prosecute failures to provide individual notice as deceptive acts or practices and to seek civil penalties of up to \$10,000 per day, per violation

Alabama Data Breach Law

- Alabama Data Breach Notification Law – Effective May 1, 2018
 - Organizations that acquire or use personal information must implement reasonable security measures.
 - Requires proper disposal of sensitive data (“sensitive data” includes any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional” and an individual’s health insurance policy number, when combined with a person’s name).
 - Requires that a breach must be likely to result in harm to affected resident to trigger notification obligations.
 - Third party agents maintain, store or process sensitive data are: (i) subject to same security requirements as covered entities; and (ii) must notify covered entities ASAP but no more than 10 days following a breach or “reason to believe a breach occurred.”
 - Violation of the notification provisions is deemed an unlawful trade practice under the Alabama Deceptive Trade Practices Act. Civil penalties of up to \$500,000 per breach. AG may also bring an action for actual damages on behalf of any affected individuals, plus attorney fees and costs.

South Dakota Data Breach Law

- South Dakota Data Breach Notification Law – Effective March 21, 2018
 - Breach is limited to unencrypted computerized data and does not apply to paper records.
 - Broad definition of “personal information” and “protected information” – SSN, state-issued ID nos., bank account numbers in combination with routing numbers, health information, employer issued ID#s in combination with passwords or biometric data when combine with a person’s name.
 - “Protected Information” includes usernames and passwords permitting access to online accounts, and account, credit, or debit numbers in combination with password or PIN.
 - If no risk of harm, no notice to affected individuals, but still must notify state AG.
 - Must notify consumer reporting agencies regardless of the size of the breach.
 - AG can prosecute failures to provide notification and seek civil penalties of up to \$10,000 per day, per violation.

State Attorneys General

- Massachusetts – Equifax litigation
 - Sept. 2017 – Announced that hackers exploited a vulnerability in a website application to gain access to names, Social Security numbers, addresses, and other personal data on its network.
 - Sept. 19, 2017, MA AG files suit against the company.
 - Alleges that consumers' information was exposed and made vulnerable to intruders because Equifax relied on certain open-source code that it knew or should have known was insecure and subject to exploitation.
 - Alleges that security patches allegedly available and known to Equifax in March 2017, did not implement such fixes until at least July 30, 2017.
 - Alleges that failure to patch resulted in allowing hackers to steal the personal information.
 - Alleges that Equifax delayed providing consumers and MA regulators with notice of the breach until Sept. 7, 2017, and failed to assist consumers in protecting themselves from the consequences of the breach through offering free security freezes, free credit and fraud monitoring for more than one year, and other measures.

California Consumer Privacy Act of 2018

- Three major components provide consumers with the right:
 1. To ask companies to disclose personal data collected;
 2. To demand personal data not be shared with third parties for business purposes; and
 3. To sue or fine companies that violate the law.
- Requires 5% of signatures of votes cast in the preceding gubernatorial election (approximately 366,000 signatures).
- Verification is due by June 28, 2018.



SECTION 6

CONGRESSIONAL ACTIVITIES

Congressional Focus on Privacy and Data Security

- Breach Notification Bill
 - Data Acquisition and Technology Accountability Act
- Social Media Targeted Legislation
 - Customer online notification for stopping edge-provider network transgressions
 - Social Media Privacy and Consumer Rights Act
- A bill that would require the FTC to establish privacy protections for online edge providers

Q&A



Thank you for running in the 2018 Technology May-rathon with us.

We would be pleased to answer your questions.

The Q&A tab is located on the bottom right hand side of your screen. Please type your questions in the space provided and click Send.

Morgan Lewis Technology May-rathon 2018

Morgan Lewis is proud to present Technology May-rathon, a series of tailored webinars and in-person programs focused on current technology-related issues, trends, and legal developments.

This year is our 8th Annual May-rathon and we are offering over 25 in-person and virtual events on topics of importance to our clients including issues of privacy and cybersecurity, new developments in immigration, employment and tax law, fintech, telecom, disruptive technologies, issues in global tech and more.

A full listing and of our tech May-rathon programs can be found at <https://www.morganlewis.com/topics/technology-may-rathon>

INSERT mlglobaltech graphic
Be sure to tweet [#techMayrathon](#)

Morgan Lewis

Biography



Greg T. Parks

Philadelphia

T +1.215.963.5170

F +1.215.963.5001

Gregory T. Parks co-chairs Morgan Lewis's privacy and cybersecurity practice and retail practice, counseling clients in retail, financial services, and other consumer-facing industries. With a focus on privacy, data security, and consumer and compliance issues, Greg advises companies in areas related to privacy and data security, class action, loyalty and gift card programs, payment mechanisms, product liability, antitrust, mortgage law, and commercial disputes. He also handles all phases of litigation, trial, and appeal work arising from these and other areas.

Morgan Lewis

Biography



**Ronald W.
Del Sesto, Jr.**

Washington, DC

T +1.202.373.6023

F +1.202.373.6421

Ronald W. Del Sesto, Jr. is a partner in the telecommunications, media, and technology (TMT) practice group. Ron's practice concentrates on the representation of 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 TMT sectors.

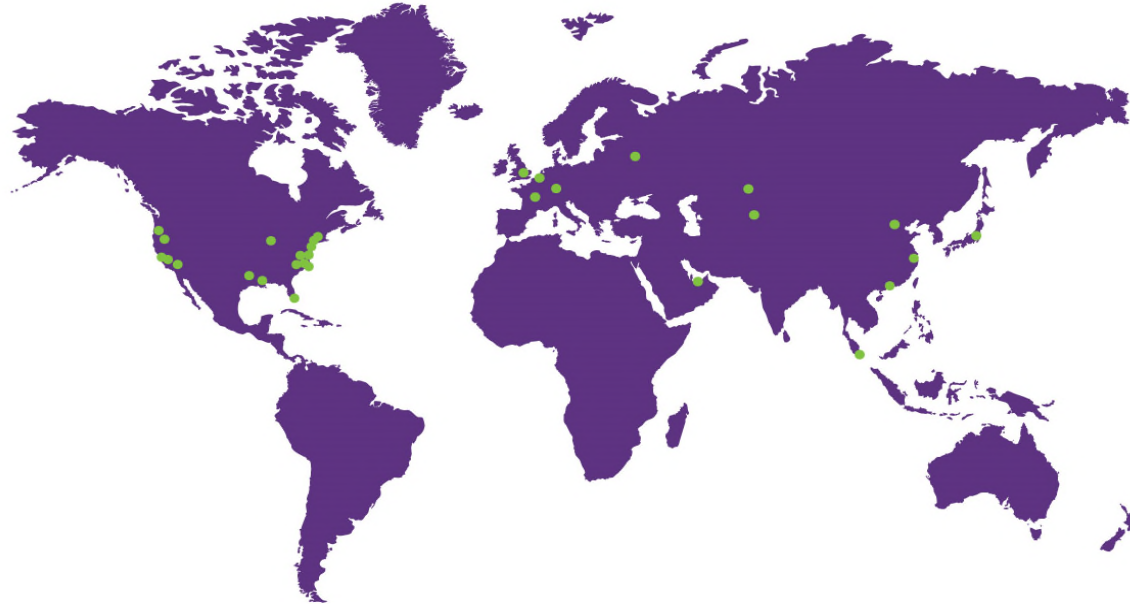
Morgan Lewis

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

THANK YOU

© 2018 Morgan, Lewis & Bockius LLP
© 2018 Morgan Lewis Stamford LLC
© 2018 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.

Morgan Lewis