Morgan Lewis

FCC & FTC DEVELOPMENTS AND RELATED DATA PRIVACY AND SECURITY ISSUES

TECHNOLOGY MAY-RATHON

Ronald W. Del Sesto, Jr. and Gregory T. Parks

May 5, 2016

Outline of FCC Update

- FCC Forfeiture Authority
- Statutory Provisions Underlying the Federal Communications Commission's (FCC) Privacy and Data Security Authority
- FCC's Open Internet Order
- Terracom and YourTel Notice of Apparent Liability
- FCC's Privacy and Data Security NPRM

SECTION 01

FCC FORFEITURE AUTHORITY

STATUTORY PROVISIONS RELATED TO PRIVACY AND DATA SECURITY

The FCC's Forfeiture Authority

- Section 503(b)(1) of the Act states that any person who willfully or repeatedly fails to comply with any provision of the Act or any rule, regulation, or order issued by the FCC, shall be liable to the United States for a forfeiture penalty.
- Section 503(b)(2)(B) of the Act empowers the FCC to assess a forfeiture of up to $160,000 against a common carrier for each willful or repeated violation of the Act or of any rule, regulation, or order issued by the FCC under the Act.
- For a violation to be willful, it need not be intentional.
- The FCC must take into account "the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."
- The FCC has established forfeiture guidelines, which establish base penalties and define criteria when exercising its discretion to issue forfeitures. The FCC may adjust forfeitures upward for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator.

Telecommunications Act Privacy and Data Security Provisions

- Section 201(b) of the Communications Act provides, in relevant part "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful.
- Section 222(a) of the Communications Act imposes a duty on every telecommunications carrier to protect the confidentiality of "proprietary information" of its customers.
- Section 222(c)(1) only permits a carrier to disclose, permit access to, or use a customer's individually identifiable CPNI to provide telecommunications services, or other services "necessary to, or used in," the carrier's telecommunications service, unless otherwise authorized by the customer or required by law.

SECTION 02

TERRACOM AND YOURTEL NAL

CUSTOMER PROPRIETARY INFORMATION

OPEN INTERNET ORDER

Terracom and YourTel – Notice of Apparent Liability (October, 2014)

Proposed forfeiture of $10 Million for:

1. Allegedly failed to properly protect the confidentiality of consumers' Proprietary Information (PI) they collected from applicants for the Companies' wireless and wired Lifeline telephone services;
2. Allegedly failed to employ reasonable data security practices to protect consumers' PI;
3. Allegedly engaged in deceptive and misleading practices by representing to consumers in their privacy policies that they employed appropriate technologies to protect consumers' PI when, in fact, they had not; and
4. Allegedly engaged in unjust and unreasonable practices by not fully informing consumers that their PI had been compromised by third-party access.

Section 222(a) and the meaning of "Proprietary Information"

- Section 222(a) of the Communications Act imposes a duty on every telecommunications carrier to protect the confidentiality of "proprietary information" (or PI) of its **customers**.
- The FCC interpreted PI broadly to encompass all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy.
- Includes personal data that customers expect their carriers to keep private, including information a carrier may possess that is not subject to the additional restrictions afforded to CPNI.
- Looks to the definition of "Personally Identifiable Information" used by the National Institute of Standards and Technology.

Section 222(a) and the meaning of "Proprietary Information" (cont'd)

- "Proprietary Information" is information such as a consumer's (i) first and last name; (ii) home or other physical address; (iii) email address or other online contact information, such as an instant messaging screen name that reveals an individual's email address; (iv) telephone number; (v) Social Security Number, tax identification number, passport number, driver's license number, or any other government-issued identification number that is unique to an individual; (vi) account numbers, credit card numbers, and any information combined that would allow access to the consumer's accounts; (vii) Uniform Resource Locator ("URL") or Internet Protocol ("IP") address or host name that identifies an individual; or (viii) any combination of the above, constitutes "proprietary information" protected by Section 222(a).
- FCC found that TerraCom and YourTel apparently violated Section 222(a) of the Act for failing to protect the confidentiality of PI that consumers provided to demonstrate eligibility for Lifeline services.

Violation of Section 201(b)

- FCC alleges that both companies engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) of the Act by failing "to use even the most basic and readily available technologies and security features and thus created an unreasonable risk of unauthorized access."
- Apparent violation of Section 201(b) of the Act by representing in their privacy policies that they protected customers' personal information, when the FCC alleges that they in fact did not.
- FCC found that both companies engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) by failing to notify all customers whose personal information could have been breached by the Companies' inadequate data security policies.

FCC's Open Internet Order (March, 2015)

- FCC's Open Internet Order:
  1. Reclassified "Broadband Internet Access Services" reclassified as a Title II Common Carrier Service;
  2. Sections 201(b) and 222 of the Communications Act apply to BIAS; and
  3. Forbears from applying Section 222 implementing rules to BIAS.
     - On appeal and decision expected soon

SECTION 03

BROADBAND AND DATA SECURITY NPRM

FCC's Broadband and Data Security NPRM

- Released April 1; Comments due May 27 and Replies Due June 27.
- Potentially applicable to voice and BIAS providers.
- The proposed new rules would:
  1. Expand the type of information subject to the FCC's Customer Proprietary Network Information (CPNI) rules to include, among other things, all forms of "Personally Identifiable Information" (PII);
  2. Impose additional obligations on providers' privacy policies;
  3. Mandate additional obligations concerning data security protections;
  4. Provide for a new right of customer access to "Customer Proprietary Information" (CPI) as well as the right to correct CPI;
  5. Impose consumer data breach notification obligations that would co-exist with current state data breach notification obligations; and
  6. Potentially prohibit certain data collection practices. The FCC also seeks comment on dispute resolution procedures including whether to prohibit BIAS providers from mandating binding arbitration in their contracts with consumers.

Customer Proprietary Information

- Customer Proprietary Information (CPI) – Two categories of information: (1) CPNI and (2) personally identifiable information (PII) acquired in connection with provision of BIAS.
- Customer Proprietary Network Information: (1) Quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service; (2) Made available to the carrier by the customer solely by virtue of the carrier-customer relationship; (3) Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; and; (4) Includes call detail information, amount of bill, service configuration, etc.
- CPNI does not include Subscriber List Information or aggregate customer information.

Customer Proprietary Information (cont'd)

- PII is defined as "any information that is linked or linkable to an individual." Information is "linked" or "linkable" to an individual if it can be used on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual.
- FCC-provided examples of PII include: name; Social Security number; date and place of birth; mother's maiden name; unique government identification numbers; physical address; email address or other online contact information; phone numbers; MAC address or other unique device identifiers; IP addresses; persistent online identifiers; eponymous and non-eponymous online identities; account numbers and other account information, including account login information; Internet browsing history; traffic statistics; application usage data; current or historical geo-location; financial information; shopping records; medical and health information; the fact of a disability and any additional information about a customer's disability; biometric information; education information; employment information; information relating to family members; race; religion; sexual identity or orientation; other demographic information; and information identifying personally owned property (e.g., license plates, device serial numbers).

Regulation of Privacy Policies

- Privacy policies would need to describe:
  - The types of CPI collected, how the BIAS provider uses and discloses each type of CPI;
  - The entities that will receive CPI from the BIAS provider and for what purpose, and
  - The customer's opt-out or opt-in rights and provide access to a simple, easy-to-access method for customers to provide or withdraw consent to use, disclose, or provide access to CPI for purposes other than the provision of broadband services. The FCC proposes that any such method will be persistently available and made available at no additional cost to the customer.

Additional Data Security Obligations

- The FCC proposes that BIAS providers, at a minimum:
  - Establish and perform regular risk management assessments and address weaknesses;
  - train personnel and affiliates that handle CPI;
  - adopt customer authentication requirements;
  - designate a senior management official responsible for implementing data security procedures;
  - establish and use robust customer authentication procedures to grant customers access to CPI; and;
  - take responsibility for the use of CPI by third parties with whom they share such information.
- Also under consideration:
  - Data minimization, retention, and destruction standards.
  - Multi-stakeholder process to develop best practices.
  - Alternatively, the FCC may prescribe specific administrative, technical, and physical conditions that must be included as part of a BIAS provider's plan to secure CPI.

Data Breach Notification Obligations

- 47 states, D.C., Guam, Puerto Rico and the Virgin Island have adopted breach notification laws.
- "Breach" is defined as any instance in which "a person, without authorization or exceeding authorization, has gained access to, used, or disclosed [CPI]." Also considering whether notice is required when a BIAS or voice provider "discovers conduct that would reasonably lead to exposure of [CPI]."

Under the proposed rules, carriers would be required to:

1. Notify affected customers of breaches of CPI within 10 days after the discovery of the breach, subject to law enforcement needs;
2. Notify the Commission of any breach of CPI within 7 days after discovery of the breach.
3. Notify the FBI and the U.S. Secret Service of breaches of CPI reasonably believed to relate to more than 5,000 customers within 7 days after discovery of the breach, and at least 3 days before notification to the customers.

SECTION 04

FTC DEVELOPMENTS

Outline of FTC Update

- FTC data security authority – *Wyndham* / *LabMD*
- EU Privacy Shield
- Internet of Things
- Regulation of credit monitoring services
- FTC Commissioner Brill Departure
- FTC / FCC "coordination"

Federal Trade Commission Statutory Authority

- Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."
- The FTC enforces data security by relying on two prohibited acts. Section 5 prohibits "unfair . . . acts" which the agency relies on when alleging an unfair practice. But in order to pursue an unfairness claim, the FTC must also establish that "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."
- Relying on the reference to a "deceptive act" in Section 5, the FTC can also allege a deceptive act when enforcing data security standards. The basis for a deceptive claim is typically an allegation by the FTC of a misrepresentation made by a company in a privacy policy, terms of service or other documentation related to data safeguards or procedures that the company will follow. Failing to adhere to the safeguards detailed in customer contracts or in related documents, or failing to follow published procedures forms the basis for a complaint based on a deceptive act.

Wyndham

- ***Wyndham***: FTC alleged that Wyndham: (1) Deceived its customers by making false or misleading representations that it had "implemented reasonable and appropriate measures to protect personal information against unauthorized access;" (2) Failed "to employ reasonable and appropriate measures to protect personal information against unauthorized access" which was unfair; and (3) Due to its actions, $10.6 million in fraudulent charges occurred resulting in substantial injury to consumers, that could not be reasonably avoided by consumers and were not outweighed by countervailing benefits to consumers or competition.
- Wyndham responded that the FTC's alleged $10.6 million harm in fraud costs ignored the fact that federal law protects users from fraudulent charges in excess of $50 and that major credit cards exempt consumers from remainder. Also, FTC failed to specify which of its practices caused alleged harm.
- District Court found FTC's evidence of consumer harm satisfied the three part test for an unfairness claim. FTC adequately demonstrated "substantial injury to consumers" that was "not reasonably avoidable" with its allegation that the breaches resulted in losses of more than $10.6 million. Rejected Wyndham's argument that the FTC's complaint did not adequately link a specific failure to the alleged harm.
- Wyndham appealed to 3rd Circuit which affirmed District Court's denial of Wyndham's motion to dismiss, affirming FTC's power to regulate, but:
  - Limited by 15 USC § 45(n) that it must: (1) cause substantial injury to consumers; (2) which is not reasonably avoidable by consumers; and (3) not outweighed by benefits.
  - Probably limited to circumstances in which the security failures are significant and many – 619,000 banana peels

Wyndham (cont'd)

- Wyndham and FTC Enter into Settlement Agreement
  - Calls for Wyndham to implement for 20 years:
  - an information security program designed to protect cardholder data, including payment card numbers, names and expiration dates
  - annual information security audits
  - safeguards in connection to its franchisees' servers
- Good news for Wyndham:
  - No money – penalties, fees, fines.
  - Very similar to existing PCI-DSS
- Good news for FTC:
  - Authority to regulate remains intact
  - Can still make an example of Wyndham if program violated

LabMD

- FTC generically alleged inadequate data security leading to two incidents disclosing names, dates of birth and social security numbers of LabMD's for 9,300 patients.
- Recognizes authority, but like *Wyndham*, limits to "substantial consumer harm."
- "At best, the FTC has proven the 'possibility' of harm, but not any 'probability' or likelihood of harm."
- Rejects FTC's arguments about:
  - "Risk of identity theft" as harm
  - Exposure of data as harm in itself
  - Future risk of harm as harm
- Case dismissed, but FTC undaunted – pursuing appeal

Reconciling *Wyndham* and *LabMD*

- Harm matters – FTC's jurisdiction would seem to be limited to those circumstances in which there is consumer harm
- Details matter – FTC needs to show specifics of what was wrong
- Scope matters – needs to be large to be "unfair"
- The law matters – 15 USC 45(n) limits FTC authority where consumers could avoid harm or there is benefit of the practice
- Settlement with FTC is generally best option

Privacy Shield

- FTC heavily involved in negotiation of Privacy Shield
- Given history on Safe Harbor, can expect more robust enforcement by FTC of Privacy Shield
- Approval facing challenges in EU. Still believe it is likely, if somewhat delayed

Internet of Things

- Connected devices proliferating at an explosive rate

- FTC taking the actions it usually takes before promulgating regulations:
  - Held a workshop
  - Announced an interest
  - Commissioners commenting publicly:
    - Commissioner Ohlhausen calls for IOT regulations on health care and automotive
    - Commissioner McSweeney saying FTC has the tools it needs

- Likely to track other basic pronouncements:
  - No misleading statements
  - Reasonable security
  - FTC would prefer "privacy by design"

Regulation of Credit Monitoring Services

- Injunction against Lifewatch follows similar action against LifeLock last year.
- Expansive promises by credit monitoring companies
- Relevant as privacy lawyers are lead consumers of these services

Commissioner Brill Departure

- Significant focus on privacy and data security agenda. Will continue.
- Now two openings on Commission. One since last August.
- Implications for Privacy Shield?

FTC / FCC Coordination

- FTC asked FCC to require "unlocking" set top boxes

- Headline: "FCC Chief Denies Superhero Rivalry with FTC on Privacy."
  - Promoting coordination / downplaying competition
  - Complementary strengths

Other Privacy Issues

- Spokeo / PF Chang's / Niemann Marcus on damages.

- Hot data breaches this Spring:
  - W2 fishing scam
  - Ransom denial of service attacks
  - Password hopping

- Debate continues over government access to computers and devices

Upcoming May-Rathon Webinars

- **Innovating in a World of Changing Spectrum Regulation (5/11/2016)**

  The FCC makes rules for providers and devices that use nongovernment radiofrequency spectrum in the United States. This session will cover what service, device innovators, manufacturers, and their financial investors should consider as they navigate the laws and FCC requirements that apply to radio spectrum, both today and in the future.

- **Be Prepared for the New EU Data Regulation (5/12/2016)**

  Join us to discuss key aspects of the new EU General Data Protection Regulation, which is due to take effect in 2018 for businesses with European operations or customers. Our speakers will provide insight from the United Kingdom, Germany, and France and will give practical guidance on how to prepare for the new data privacy rules.

- **EAR Encryption Regulations: A New Enigma Machine or a Mystery Wrapped in a Riddle (5/18/2016)**

  US encryption controls are complex, and the requirements are not easily identified by clients. This webinar will decipher encryption regulations and provide tips on company encryption registration, classification of products, reporting, and applicability of the regulatory requirements to a range of activities, such as cloud-based services.

- **Mid-Year Telecom/Media Regulatory and Legal Update (5/19/2016)**

  Many corporate transactions involve conditions governed by regulations specific to telecommunications or media. This session will identify due diligence and deal structure issues, required approvals for mergers and acquisitions (M&A) and financing, considerations based on foreign (or other) ownership, and key compliance issues.

- **Don’t Get Tricked by the Click (5/31/2016)**

  Join us for an update on developments with e-commerce clickwrap agreements & arbitration clauses.

Biography

Ronald W. Del Sesto, Jr. is a partner in the Telecommunications, Media and Technology (TMT) 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.

Ronald W. Del Sesto, Jr.
Washington, D.C.
T +1.202.373.6023
F +1.202.373.6421
rdelsesto@morganlewis.com
Twitter: @rdelsesto

Biography

Gregory Parks
Philadelphia
T +1.215.963.5170
F +1.215.963.5001
Gregory.parks@morganlewis.com

Gregory T. Parks co-chairs Morgan Lewis's privacy and cybersecurity practice and our retail practice, counseling clients in retail, financial services, and other consumer-facing industries. With a focus on privacy, data security, 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.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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

Morgan Lewis

THANK YOU