Morgan Lewis

PRIVACY AND DATA SECURITY: THE EVOLVING ROLES OF THE FCC AND FTC

Ron Del Sesto and Greg Parks
May 14, 2015

Outline

- Statutory Provisions Underlying the Federal Communications Commission's (FCC's) Privacy and Data Security Authority
- Recent FCC Enforcement Actions
- The Privacy and Data Protection Implications of the FCC's Recent Net Neutrality Order
- Statutory Provisions of the Federal Trade Commission's (FTC's) Privacy and Data Security
- Brief Consideration of *Wyndham* Litigation
- *In the Matter of HTC America Inc.*
- *In the Matter of Nomi Technologies, Inc.*
- Designing a Cybersecurity Risk Management Program

ENFORCEMENT OF PRIVACY AND DATA SECURITY BY THE FEDERAL COMMUNICATIONS COMMISSION

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 Consumer Proprietary Network Information (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.

Customer Proprietary Network Information

- Quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service;
- Made available to the carrier by the customer solely by virtue of the carrier-customer relationship;
- Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; and
- Includes call detail information, amount of bill, service configuration, etc.
- CPNI does not include Subscriber List Information or aggregate customer information.

FCC Enforcement Actions Directed at Privacy and Data Security Violations

- AT&T Pays $25 Million Civil Penalty Pursuant to a Consent Decree (April 2015)
- FCC Issues a Notice of Apparent Liability Against TerraCom and YourTel America and Proposes a $10 Million Fine (October 2014)
- Verizon Enters into a $7.4 Million Consent Decree (September 2014)
- Sprint Enters into a $7.5 Million Consent Decree (May 2014)
- FCC Issues a Notice of Apparent Liability Against Dialing Services and Proposes a $2.944 Million Fine (May 2014)

TerraCom and YourTel Notice of Apparent Liability (NAL)

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" pursuant to a National Institute of Standards and Technology publication.

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.

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.

The FCC's Forfeiture Analysis as Applied to TerraCom and YourTel

- The FCC notes that neither the forfeiture guidelines nor its case law establishes a base forfeiture for violations of Section 222(a).
- The FCC starts with the principle that the protection of consumer PI is a fundamental obligation of all telecommunications carriers.
- Based on forfeitures issued for violations of the CPNI rules, and the severity of the data security violations in this case, the FCC establishes a base forfeiture amount of $29,000 for violation of 222(a).
- For violations of 201(b), the FCC in other contexts has established a base forfeiture of $40,000 for each action that is unjust and unreasonable and proposes a forfeiture in the amount of $1.5 million.

Dialing Services, LLC Notice of Apparent Liability

- In 2012, the FCC investigates Dialing Services offerings.
- The FCC finds that in a period of 3 months, Dialing Services had placed 4.7 million non-emergency calls to cellular telephone numbers in violation of the Telephone Consumer Protection Act (TCPA).
- FCC issues a Citation and warns Dialing Services of possible forfeiture penalties if the cited conduct continues where Dialing Services could be subject to a forfeiture in the amount of $16,000 for each violation of the TCPA.
- In June, 2013, the FCC initiated another investigation of Dialing Services finding that the company had made 184 calls in violation of the TCPA.
- FCC issues the Notice of Apparent Liability in the amount of $2.944 million.

The Privacy and Data Protection Implications of the FCC's Recent Net Neutrality Order

- "Broadband Internet Access Services" reclassified as a Title II Common Carrier Service.
- Sections 201(b) and 222 of the Communications Act apply to "Broadband Internet Access Services."
- Forbears from applying implementing rules to "Broadband Internet Access Services."

THE FEDERAL TRADE COMMISSION'S ENFORCEMENT OF PRIVACY AND DATA SECURITY

FTC Privacy and Data Security

- Statutory Provisions Related to Privacy and Data Security
- The *Wyndham* Litigation
- In the Matter of *HTC America Inc.*
- In the Matter of *Nomi Technologies, Inc.*

FTC 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 Litigation

- Wyndham was charged in 2012 for "unfair and deceptive acts" arising from alleged data breaches in its franchisees' computer systems.
- FTC pled both unfairness and deceptive acts against Wyndham but it is the unfairness grounds that has brought most of the controversy.
- Wyndham argued that the FTC's substantive unfairness standards for data security exceeded the Agency's authority.
- Wyndham also argued that there was no fair notice as the FTC had not issued any formal regulations governing data security requirements.
- Wyndham argued that the "reasonableness" standard, standing alone, is ambiguous and does not provide businesses with any specific guidance to achieve a data security safe harbor unlike what other agencies have done.
- FTC responded that the FTC Act provided the Agency with a baseline authority to act in cases of unfairness where it can prove substantial harm to consumers.
- FTC responded that its informal guidance is enough to put businesses on notice of what is required to meet the "reasonableness" standard.

U.S. District Court for the District of New Jersey

- First, the court ruled as a matter of law that FTC Act Section 5 empowers the FTC to regulate data security.
- Second, the court found that the FTC does not need to formally publish rules and regulations governing unfair data security practices since the prohibitions in Section 5 are flexible.
- Third, the court held that the FTC had sufficiently alleged how Wyndham's data security practices were unfair and deceptive.
- The court granted leave for an interlocutory appeal to the Third Circuit Court of Appeals on two certified questions:
  (1) Whether the FTC can bring an unfairness claim involving data security under Section 5 of the FTC Act; and
  (2) Whether the FTC must formally promulgate regulations before bringing its unfairness claim under Section 5 of the FTC Act.

Importance of *Wyndham*

- For the last 15 years, FTC has taken the self-appointed lead on data security and this was the first case to challenge the scope of its jurisdiction.
- Prevailed in the absence of defining uniformly acceptable data security practices.
- Open questions remain:
  1. "Substantial injury to consumers";
  2. Continuing need for legislation; and
  3. Future of the FTC's case-by-case approach.

In the Matter of HTC America Inc.

- FTC alleged both "unfair and deceptive acts or practices affecting commerce."
- FTC charged HTC with failing to employ "reasonable security measures" when customizing software used in certain mobile devices running the Android and Windows Phone mobile operating systems.
- The FTC alleged that when HTC customized Android software on its devices and shipped devices with pre-installed software, HTC introduced numerous vulnerabilities that would not have been present but for HTC's customizations.
- The FTC also alleged that HTC introduced vulnerabilities into devices when customizing devices for carriers like Sprint and AT&T.
- HTC's failure to discover these vulnerabilities by not implementing a comprehensive security program into its operations constitutes an unfair practice according to the FTC complaint.

In the Matter of HTC America Inc. (cont'd)

- Regarding the "deceptive act" prong of Section 5, the FTC alleged that statements made in HTC's user manuals and in HTC's pre-installed software were false due to the inherent vulnerabilities introduced to HTC devices by HTC.
- Consent Decree Terms:
  1. Release software patches to fix the vulnerabilities;
  2. Implement a comprehensive written security program designed to address security risks during the development of new devices as well as existing covered devices;
  3. Undergo an independent security assessment every other year for the next 20 years; and
  4. Protect the security, confidentiality, and integrity of "covered information" collected by HTC or input into, stored on, captured with, accessed, or transmitted through a covered device.

In the Matter of Nomi Technologies, Inc.

- Nomi Technologies uses its own sensors and its retail clients' Wi-Fi access points to collect media access control (MAC) address broadcast by a mobile device when it searches for Wi-Fi networks.
- Nomi uses the information it collects to provide analytics reports to its clients about aggregate customer traffic patterns.
- Nomi provided a means to opt-out exclusively on its Website.
- Nomi's privacy policy provided: "Nomi pledges to… Always allow consumers to opt out of Nomi's service on its website as well as at any retailer using Nomi's technology."

Nomi Technologies Consent Decree

- Nomi agreed not to misrepresent in any manner, expressly or by implication:

  (A) the options through which, or the extent to which, consumers can exercise control over the collection, use, disclosure, or sharing of information collected from or about them or their computers or devices,

  or;

  (B) the extent to which consumers will be provided notice about how data from or about a particular consumer, computer, or device is collected, used, disclosed, or shared.

DESIGNING A CYBERSECURITY RISK MANAGEMENT PROGRAM

Cybersecurity Basics

- Implementing
  - Malware Protection
  - Network Security
  - Secure Configuration
  - Managing User Privileges
  - Remote and Mobile Access to Enterprise Systems
  - Removable Media
  - Monitoring
  - Supply Chain and Vendor Management

Cybersecurity Risk Management Overview

- First, management must perform risk analysis;
- Second, leadership must take action to instill best practices in the organization; and
- Third, businesses must be prepared to detect and respond to cyber events both internally and externally.

Cybersecurity Risk Management

- Perform a Risk Assessment
  - What information assets are critical to your business?
  - What obligations do you have under relevant law and by contract?
  - Who poses threats to these assets?
  - What form could the threat take?
  - What impact could an attack have on your business?
- Ongoing Planning
  - Managing cybersecurity risks on an ongoing basis
  - Reviewing and testing effectiveness of your controls
  - Monitoring and acting on information you receive from your controls
  - Staying current on the latest threats
  - Cyber risk insurance
- Response Plans
  - Legal compliance
  - How would your organization continue to do business in the event of a cyber attack?

Information Security Program

1. Identify the information that requires safeguarding.

2. Consider potential threats, vulnerabilities, and risks to the security of such information.

3. Establish and maintain appropriate policies and administrative, physical, and technical controls to address the identified threats, vulnerabilities, and risks to the security of safeguarded information.

4. Consider the security of safeguarded information when such information is accessible to third parties.

5. Respond internally and externally to discovered breaches.

6. Periodically review and update policies and controls for the security of safeguarded information.

Continued Legal Education

We are pending CLE for the following states:

- California
- Florida
- Illinois
- New Jersey
- New York – **CODE SP805**
- Pennsylvania
- Texas
- Virginia

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) 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.

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 our 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.

ASIA

Almaty
Astana
Beijing
Singapore
Tokyo

EUROPE

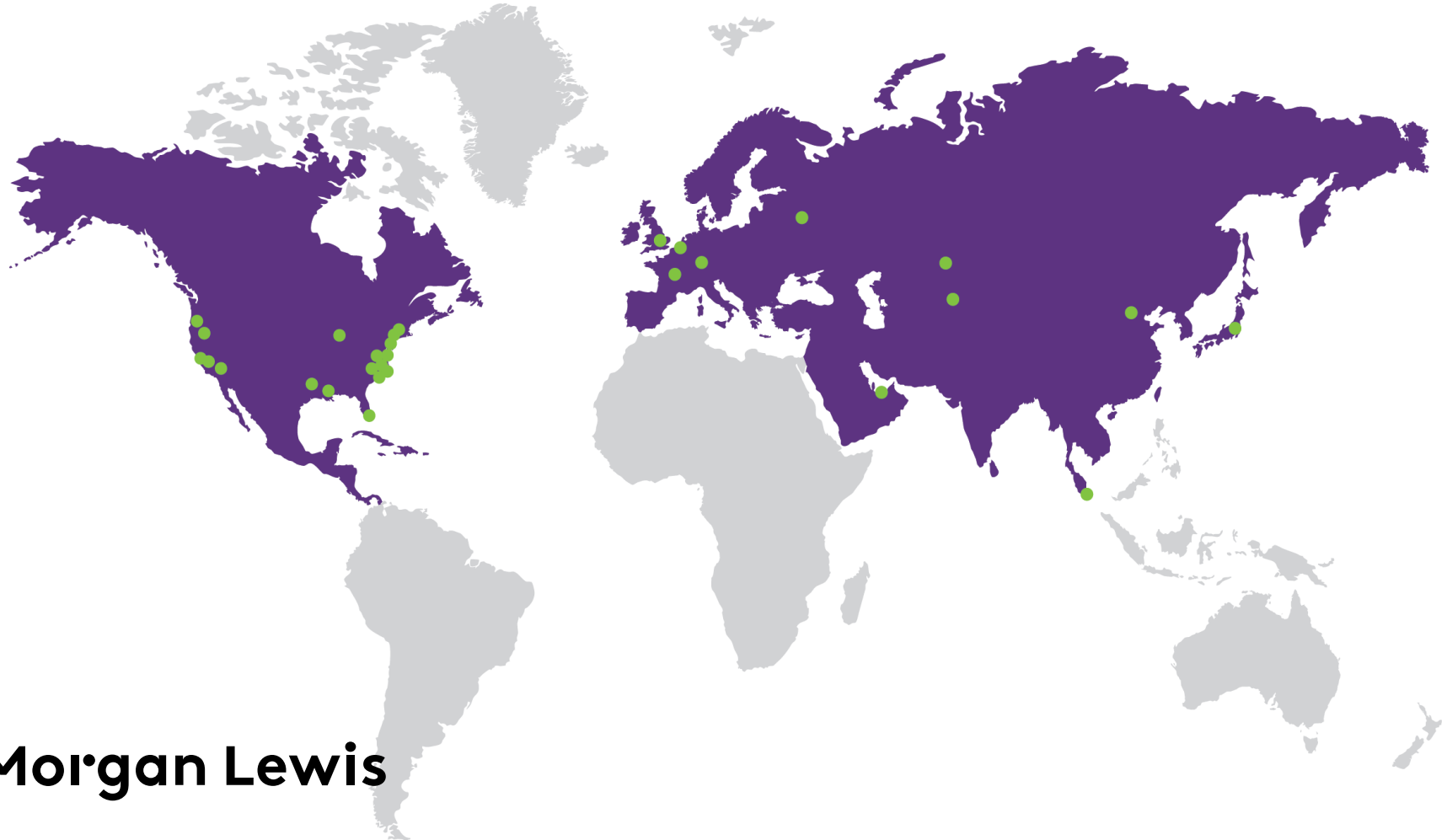
Brussels
Frankfurt
London
Moscow
Paris

MIDDLE EAST

Dubai

NORTH AMERICA

Boston
Chicago
Dallas
Harrisburg
Hartford
Houston
Los Angeles
Miami
New York
Orange County
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Silicon Valley
Washington, DC
Wilmington



Morgan Lewis

THANK YOU