Wiley Rein LLP

# PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | May 2015

## Introduction

With privacy and data security in the news almost every day, this month's issue of *Privacy in Focus* addresses recent and ongoing enforcement activity in several settings. Bruce L. McDonald looks at the Federal Trade Commission's (FTC) most recent enforcement activity, addressing the tricky area of consumer tracking. Megan L. Brown, Mark B. Sweet, and C. B'anca Glenn look at the most important ongoing FTC action—the longstanding *Wyndham* litigation—and the most recent steps in that ongoing and incredibly important proceeding. Scott D. Delacourt, Shawn H. Chang, and Megan L. Brown look at the latest entrant to the enforcement universe—the Federal Communications Commission—and its latest enforcement proceeding.

As always, we are appearing at various events, with more to follow over the coming months. I testified this month at a hearing for the National Committee on Vital and Health Statistics on the interplay between HIPAA and the activities of financial institutions. Please let me know if you have questions about any of these events. If you have issues you'd like us to address in future editions of *Privacy in Focus*—or areas where we can be helpful to you on these issues—please let me know at knahra@wileyrein.com or 202.719.7335. Thank you for reading. ■

Kirk Nahra, Privacy Practice Chair

ALSO IN THIS ISSUE



## FCC, Again, Establishes Data Security Requirements by Consent Order

For the second time, the Federal Communications Commission (FCC or Commission) has taken enforcement action predicated on its purported authority over data privacy and security allegedly found in Section 201(b) of the Communications Act. Eschewing rulemaking, the agency's action comes in the form of an Order and Consent Decree (Order) with a major wireless carrier. In addition to imposing a $25 million civil penalty, the FCC announced a new category of protected data, "Personal Information," which must be safeguarded by entities subject to Title II of the Communications Act (the Act).

The April 8, 2015 Order settles an investigation into a data breach at the carrier's call centers in Mexico, Colombia, and the Philippines. The Order addresses disclosure of account-related data known as customer proprietary network information (CPNI) and whether the safeguards in place were "just and reasonable" under Sections 201(b) of the Act. The data at issue included customers' CPNI, names, and at least the last four digits of their Social Security numbers. The Order indicates that such information could be used to place handset unlocking requests and sold to third parties.

continued on page 3

# Court of Appeals Raises Doubts about the FTC's Cybersecurity Approach in *Wyndham*

After a series of Russian cyber-attacks on Wyndham-affiliated hotels, the Federal Trade Commission (FTC or Commission) sued various Wyndham entities, claiming that their allegedly deficient data security practices violated Section 5(a) of the Federal Trade Commission Act (FTC Act), which prohibits "unfair or deceptive acts or practices." Wyndham fought back, and now the FTC's action is being reviewed by the U.S. Court of Appeals for the Third Circuit, in *FTC v. Wyndham*, No. 14-3514. The fundamental issue raised is whether, in the absence of regulations or applicable security standards, the FTC is empowered to police the general data security practices of American businesses by bringing enforcement actions after a breach.

The appeals court is reviewing a District Court decision that sustained the FTC's approach. Briefing has been extensive, with numerous *amicus* briefs submitted. Recent supplemental briefing signals court skepticism about the FTC's approach. But the agency remains committed to its enforcement, warning corporate general counsels to be vigilant and heed the FTC's guidance.

### Third Circuit Skepticism

Shortly before oral argument, the Third Circuit asked the attorneys to address supplemental questions. These questions signal some skepticism about the FTC's approach and potential discomfort with courts being asked to assess the substantive reasonableness of corporate data security practices. The court posed two questions concerning the FTC's authority over unfair cybersecurity practices:

(1) Has the FTC previously determined that unreasonable cybersecurity practices are "unfair," using the procedures of the FTC Act; and,

(2) Assuming it has not, "is the FTC asking the federal courts to determine that unreasonable cybersecurity practices are 'unfair' in the first instance, and if so, can the courts do so in this case brought under 15 U.S.C. § 53(b)?"

continued on page 4

# FTC Tracking Settlement Relies on an Implied Website Claim

The Federal Trade Commission (FTC or Commission), on April 23, announced a consent order settlement with Nomi Technologies, Inc. (Nomi) resolving, subject to public comment, the Commission's assertion that representations made in Nomi's website privacy policy were false and therefore Nomi had violated Section 5 of the Federal Trade Commission Act. Two of the five commissioners dissented, writing that the circumstances did not warrant an FTC enforcement proceeding.

The Commission's enforcement initiatives have long maintained that commercial privacy policies must not be false or deceptive. Here, however, the FTC partly relied on an "implied representation," a move that may merit note by firms that maintain website privacy policies.

### The Nomi Privacy Policy

As understood by the FTC, Nomi provides technological services that allow retailers to track consumers' movements around their stores. This is accomplished by monitoring media access numbers of consumers' mobile devices. Those numbers were processed (hashed), and the detected location and movement information was assembled in analytic reports on "aggregate consumer traffic patterns" that were provided to client retailers. No data was provided on individual mobile devices or individual consumers.

Nomi perceived that nevertheless some mobile device users might be troubled by the tracking of their movements in this way. During the relevant period, Nomi's website privacy policy contained a "pledge" to "always allow consumers to opt out of Nomi's service on its website as well as at any retailer using Nomi's technology."

The flaw precipitating the FTC enforcement initiative was that, although Nomi enabled consumers to opt out on its website, Nomi "did not provide an opt-out mechanism at its clients' retail locations." Thus, the

continued on page 5

## "Personal Information" Covered

The relief imposed by the Order is instructive for telecommunications companies subject to Title II and the FCC's CPNI rules. The Order imposed both a $25 million civil penalty and mandates a compliance plan that includes implementation of new practices designed to protect CPNI and "Personal Information," a newly-defined term that means:

"(1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver's license number or other government-issued identification card number; or (C) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account."

Specific requirements of the compliance plan include:

- Appointing a senior compliance manager who is privacy certified;
- Conducting a privacy risk assessment;
- Implementing an information security program;
- Preparing a compliance manual; and
- Employee training.

The Order comes on the heels of a $10 million Notice of Apparent Liability for Forfeiture (NAL) issued to TerraCom, Inc. (TerraCom) and YourTel America, Inc. (YourTel) in October 2014, a case that signaled an FCC interest in data privacy and security beyond the scope of the agency's CPNI rules. There, the FCC alleged that storing proprietary information collected from consumers in an easily accessible format on the Internet violated Section 201(b) as an "unjust and unreasonable practice." Citing this NAL – non-final agency action taken by the Enforcement Bureau that has not ripened into a Forfeiture Order by the Commission – the Order states that "Section 201(b) applies to carriers' practices for protecting [personally identifiable information] (PII) and CPNI."

In addition, the Order states that Section 222 of the Act and the CPNI rules (together the CPNI provisions) require carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI" and to notify law enforcement within seven business days of a breach. Notably, the Order reflects that the enforcement target admits, "[f]or the purposes of th[e] Consent Decree only," that the actions subject to the FCC investigation violated the CPNI provisions. The Order contains no similar statement with respect to Section 201(b).

## Aggressive FCC Enforcement

Coming after enforcement action against YourTel and Terracom, the Order signals a growing FCC interest in enforcing a broad concept of data privacy and security that goes beyond the scope of the agency's existing CPNI rules. It also suggests the FCC will continue to be aggressive in the exercise of its broad asserted enforcement authority over data privacy and security, grounded in section 201(b).

Furthermore, the Order injects new uncertainty into the current Congressional debate over the creation of a national data security and breach notification regime enforceable by a single federal regulatory authority. The Order's definition of "Personal Information," the high forfeiture level, and the creation of a new category of protected data through adjudication absent rulemaking all touch on issues being addressed by a draft bill introduced by Representatives Marsha Blackburn (R-TN) and Peter Welch (D-VT). Given that the legislation would shift the FCC's data security and breach notification jurisdiction to the Federal Trade Commission without a grant of rulemaking authority, the Order not only outlines the potential scope of power being lost and gained by the agencies under the bill, it could also shape lawmakers' views on the standards that should apply under a new national regime.

For more information on FCC enforcement and evolving data security requirements, please contact:

Scott D. Delacourt
202.719.7459
sdelacourt@wileyrein.com

Shawn H. Chang
202.719.4456
schang@wileyrein.com

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

With these questions, the court asks the FTC to defend its choice to police cybersecurity through case-by-case adjudication in federal court, rather than through regulatory methods like agency adjudication. Section 13(b) of the FTC Act permits the FTC to seek preliminary and permanent injunctions in federal court, and the FTC has chosen federal court action here to take advantage of the additional remedies available, including equitable monetary remedies, such as disgorgement or restitution. At oral argument, the court asked counsel to file supplemental briefing on these questions. Those briefs shed light on the dispute and the FTC's position.

## The FTC's "Previous Determinations"

With respect to the Third Circuit's first question—whether the FTC has found unreasonable cybersecurity practices to be unfair under the FTC Act's procedures—the parties strongly disagree. Not surprisingly, the FTC argues that it previously has adequately addressed and provided guidance about the agency's expectations. The FTC cites its order refusing to dismiss the pending *LabMD* administrative enforcement proceeding, the fact that it has voted to issue over 20 complaints for inadequate data protection as unfair practices, the Commission's guidance documents, and its prior testimony before Congress on inadequate data security. The FTC recognized that complaints are not binding precedent, but noted that complaints have value as reasoned guidance.

In contrast, Wyndham's supplemental brief argues that the "the FTC has not declared unreasonable cybersecurity practices 'unfair' through the procedures in the FTC Act, 15 U.S.C. §§ 41-58." Wyndham argues that the Commission's order in *LabMD* was not a final order and the Commission "cannot transform complaints and consent decrees into rules and adjudications." Citing the court's statements from oral argument, Wyndham pointed out that "the FTC has never directed the public to look to complaints or consent decrees for guidance, and those are not the typical sources which counsel would turn in advising clients." For these reasons, Wyndham argues that its earlier practices have not and cannot be deemed "unfair" under the FTC Act.

## Appropriateness of this Judicial Review

Confronted with the Court's skepticism about the use of federal court rather than agency procedure, both the FTC and Wyndham agree that the court need not address the question of whether this case is properly before a federal court. Both parties are committed to having a federal court decide the issues, for different reasons.

The FTC seeks to preserve a procedural vehicle for litigating its cases, and vigorously defends its authority to choose its forum. It argues that Congress permits the FTC to enforce the FTC Act through either administrative procedures or litigating in federal courts under Section 13(b). The FTC claims broad discretion to determine which cases are suited for federal court versus those that should go through the administrative process. The FTC emphasizes that federal district courts are amply equipped to handle this sort of case, as the questions presented are not more difficult than others addressed by the courts, and Section 13(b) has been applied to many complex and "non-routine" cases like the dispute here.

Wyndham likewise desires to have its day in court, or at least to avoid the FTC's adjudicative process. Wyndham agrees that the Third Circuit need not address the jurisdiction question, arguing that the issue was not raised by either party, the FTC's authority under Section 13(b) is not jurisdictional here, and that finding against the FTC on this issue would create a circuit conflict. But if the court were inclined to find a procedural problem with the FTC's unfairness claim, Wyndham urges the court to hold the FTC to its choice of litigation strategy. As Wyndham describes it, the FTC traded a favorable forum—its own administrative law judges, more favorable rules, and Commission review of the decision—for broader potential remedies in the form of monetary penalties.

In urging the Court to bring some closure to this dispute, Wyndham casts doubt on the utility and fairness of administrative adjudication here. The alleged conduct is five years old, and, "[i]in light of the advanced nature of this case and the substantial burdens Wyndham has already incurred, the FTC should not be permitted to start litigation anew." Wyndham also questions whether it "could receive a fair hearing if this case were litigated at the FTC. Before last year, no private litigant had prevailed in the FTC's administrative courts in nearly twenty years."

At bottom, Wyndham argues that if the Court finds "that the FTC lacked authority to bring its unfairness claim" in federal court, it should dismiss that claim with prejudice

continued on page 5

*Court of Appeals Raises Doubts about the FTC's Cybersecurity Approach in Wyndham* continued from page 4

and not allow the FTC to re-file its unfairness claim in its own administrative courts." And if it were inclined to let the FTC take another shot at Wyndham, "[a]t the very least, the Court should hold that the FTC cannot pursue an unfairness claim against Wyndham without first promulgating a rule declaring unreasonable cybersecurity practices unfair."

## FTC Will Remain the Cop on the Beat

The FTC's aggressive policing of data and cybersecurity practices has raised controversial legal issues about agency authority and process. While the Third Circuit's much anticipated decision may bring some clarity to the breadth of the FTC's authority and the proper FTC procedures for regulating corporate cybersecurity, the FTC has made clear it is not going to be shy in acting to protect consumers.

The agency emphasized that it is the "the only consumer protection agency that is able to proceed against companies that accept confidential data from their customers and then fail to take steps to protect that data." At oral argument, the FTC made clear that all businesses must be on notice of the Commission's approach to adequate cybersecurity practices, stating that "any careful general counsel would be looking at what the FTC is doing, [as the FTC] has broad ranging jurisdiction [over the private sector] and undertakes frequent actions against all manner of practices and all manner of businesses."

The FTC has underway several efforts regarding data security, cybersecurity, and privacy. Businesses should be vigilant in their approach, and mindful of the FTC's watchful eye.

For more information on the Wyndham litigation and FTC data security policy please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Mark B. Sweet
202.719.4649
msweet@wileyrein.com

C. B'anca Glenn
202.719.3733
cglenn@wileyrein.com

*FTC Tracking Settlement Relies on an Implied Website Claim* continued from page 2

proposed administrative complaint alleges, the retail-locations representation as "false or misleading."

## Future Implications

The good news for tracking firms is that the FTC did not challenge the tracking practice itself or claim that notice must always be given of its use.

However, firms of all types that have privacy policies may find problematic that the Commission majority (Chairwoman Ramirez, Commissioner Brill and Commissioner McSweeny) found the quoted website language to represent that "consumers would be given notice when a retail location was utilizing Nomi's" service. The Nomi website language does not make that representation in those words. Rather, the FTC found it to be implicit in the representation that Nomi always "will allow consumers to opt out…at any retailer using Nomi's technology."

The Commission's construction would seem to rule out a business model where retailers would say nothing about Nomi's service but would allow opt outs by consumers who asked if the service was in use and then sought to opt out. Those presumably would be some of the consumers who had learned about the service from Nomi's website or some other source. The Commission's analysis does not discuss that business model, much less explain why a policy allowing such "under the counter" opt outs would be false, deceptive or unfair.

If a firm offering such a service did not want to give consumer notice at retail establishments that the service was in use, then the Commission's interpretation would suggest that such a service provider should refrain from allowing opt outs at the retail establishments. The Commission materials do not discuss that implication.

For more information, please contact:

Bruce L. McDonald
202.719.7014
bmcdonald@wileyrein.com

# SPEECHES & EVENTS

Deterring Cyber-Threats: Lessons Learned from the Sony, Target, and Other Mega Breach Incidents

**Megan L. Brown, Speaker**

FCBA and IAPP Florida Privacy and Cybersecurity Law Symposium

May 14, 2015 Jacksonville, FL

The Evolving World of Privacy and Security – What's It Mean to You?

**Kirk J. Nahra, Panelist**

HITRUST 2015

May 21, 2015 Grapevine, TX

Digital Invaders - Data Breaches: Risk and Insurance Coverage

**Laura A. Foggan, Speaker**

ACCEC 2015 Annual Conference

May 21, 2015 | Chicago, IL

HIPAA and FERPA Privacy Protections for Student Records

**Kirk J. Nahra, Speaker**

IAPP Teleconference

June 18, 2015 Teleconference

Healthcare Quarterly Update: Cybersecurity and Health Data Privacy

**Kirk J. Nahra, Speaker**

Bloomberg BNA CLE Panel Discussion

June 24, 2015 Washington, DC

## Contributing Authors


| | | |
|---|---|---|
| Megan L. Brown | 202.719.7579 | mbrown@wileyrein.com |
| Shawn H. Chang | 202.719.4456 | schang@wileyrein.com |
| Scott D. Delacourt | 202.719.7459 | sdelacourt@wileyrein.com |
| C. B'anca Glenn | 202.719.3733 | cglenn@wileyrein.com |
| Bruce L. McDonald | 202.719.7014 | bmcdonald@wileyrein.com |
| Kirk J. Nahra | 202.719.7335 | knahra@wileyrein.com |
| Mark B. Sweet | 202.719.4649 | msweet@wileyrein.com |