KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

November 3, 2014

The FCC Moves To Expand Its Data Security Regulatory Reach

The FCC fines two telecommunications companies $10 million—and faces significant internal dissent[1]

On October 24, 2014, the Federal Communications Commission (FCC) **levied a $10 million fine** against two telecommunications companies that allegedly stored unencrypted personally identifiable customer data online with no security safeguards.[2] Although the FCC has primary regulatory authority over telecommunications companies, this appears to be the first time the agency has ventured into the arena of data security enforcement and, according to FCC Enforcement Bureau Chief Travis LeBlanc, "it will not be the last."[3]

Although the proposed $10 million fine in the matter is noteworthy, just as significant is the internal dissent the FCC's actions drew from two Commissioners. Those dissents—which questioned the FCC's authority to act—must be examined in the context of the FCC's overall authority to protect consumer privacy with respect to telecommunications activities, and how the FCC's authority interacts and overlaps with that of the Federal Trade Commission (FTC).

FCC Imposes $10 Million Fine on TerraCom and YourTel America

By a 3-2 vote, the FCC decided to assess a $10 million fine on TerraCom Inc. and YourTel America Inc. for placing the personal data of up to 300,000 consumers at risk by storing Social Security numbers, names, addresses, driver's license information, and other sensitive consumer information on Internet servers that were accessible to the general public.[4] According to the FCC, TerraCom and YourTel, which share the same owners and management, collected data on consumers to demonstrate eligibility for the FCC's Lifeline program, which is a universal service fund program that provides inexpensive phone services to low-income individuals.[5] Although the companies claimed to have "technology and security features [in place] to safeguard the privacy of [] customer specific information from unauthorized access," the customer data the companies collected was allegedly accessible through the Internet between September 2012 and April 2013.[6] When reporters from the Scripps Howard News Service found these personal records through a simple Google search, they

For more information, contact:

John C. Richter
+1 202 626 5617
jrichter@kslaw.com

S. Stewart Haskins, II
+1 404 572 4687
shaskins@kslaw.com

Christopher C. Burris
+1 404 572 4708
cburris@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

John A. Drennan
+1 202 626 9605
jdrennan@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

notified the FCC.[7] After being put on notice of the security lapse, TerraCom and YourTel allegedly failed to notify all potentially affected customers, depriving those individuals of the opportunity to protect their personal information.

The FCC held that the companies' alleged failure to secure personal information constituted a violation of the companies' statutory duty under section 222(a) of the Communications Act to protect that information, as well as an unjust and unreasonable practice in violation of section 201(b) of the Act, "given that their data security practices lacked even the most basic and readily available technologies and security features and thus create[d] an unreasonable risk of unauthorized access."[8] Section 503(b)(1) empowers the FCC to order forfeiture penalties for violations of the Act, but does not specify the base forfeiture for each violation. Here, the FCC found that a base forfeiture of $29,000 per violation was appropriate, and because TerraCom and YourTel stored personal information for over 300,000 customers, the FCC noted that it *could have* fined the companies $9 billion. However, considering the "extent and gravity of the circumstances,"[9] the FCC instead decided to impose a fine of $10 million. This is the largest privacy action in the FCC's history,[10] but LeBlanc explained, "[w]hen [telecommunications companies] break [the trust of their consumers], the [FCC] will take action to ensure that they are held accountable for unjust and unreasonable data security practices."[11]

The FCC Commissioners' Dissent

Two FCC Commissioners disagreed with the FCC's decision and forfeiture penalty. The dissenting Commissioners argued that the FCC does not have authority to enforce data security regulations because no one, including the FCC, has ever interpreted the Communications Act to enforce a duty on telecommunications carriers to protect personally identifiable information ("PII"). Although section 222(a) imposes a duty on carriers to protect "proprietary information," the dissent argued that section 222(b) and (c) limited that duty to protecting "consumer proprietary network information" ("CPNI") from marketing use and disclosure to third parties. CPNI is generally defined as phone-call-related data, such as the phone numbers called and the frequency, duration, and timing of such calls;[12] on the other hand, PII encompasses personal data that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.[13] Although the FCC's decision defined section 222(a)'s "proprietary information" to include PII,[14] the dissenting Commissioners emphasized that section 222(a) should be interpreted in accordance with the other sections of the Act that restrict the use of CPNI, and that CPNI cannot be equated with PII. According to the dissenters, because section 222(a) of the Communications Act does not apply to PII, that section "was never intended to address the security of data on the Internet."[15] By imposing "never-adopted rules" that greatly broaden the reach of the Communications Act, the dissenting Commissioners stressed, the FCC ran "afoul of the fair warning rule" of due process.[16]

One of the dissenting Commissioners also noted that "it strains credulity to think that Congress intended" penalties as massive as $9 billion for telecommunications carriers, but not for other businesses that handle PII.[17] Such enormous potential penalties are particularly egregious, argued the Commissioner, considering that the FCC has penalized the same companies only hundreds of thousands of dollars for multiple violations of actual substantive rules promulgated by the FCC.[18]

The FTC and Data Privacy and Security Enforcement at the Federal Level

The FCC Commissioners' dissent highlights the fact that, at the federal level, data privacy and security enforcement has long been the primary domain of the FTC, with certain industry-specific authority held by other regulatory agencies. The FTC's general authority to regulate consumer data privacy and security issues stems from Section 5(a)(1) of the FTC Act, which restricts "unfair and deceptive trade practices"—although the FTC also has

enforcement authority with respect to other targeted privacy laws, such as: (1) the Gramm–Leach–Bliley Act, (2) the Fair Credit Reporting Act ("FCRA"), and (3) the Children's Online Privacy Protection Act ("COPPA").[19]

Although the FTC has various means of regulating data privacy and security practices, the FTC and the FCC have long acknowledged an overlap between their spheres of authority in the area of privacy, specifically as it relates to telecommunications companies. For example, in 2006 the FTC appeared before the Oversight and Investigations subcommittee of the U.S. House Committee on Energy and Commerce to discuss the issue of "pretexting" – the practice of obtaining unauthorized access to consumer telephone records through deceit.[20] During the hearing, the FTC stated that it "work[ed] closely" with the FCC to bring five cases against entities engaged in pretexting because the FCC "has jurisdiction over telecommunications carriers subject to the Communications Act."[21] More recently, in a comment filed by the FTC with the FCC regarding the regulation of Internet broadband providers, the FTC stated, "[t]he FTC welcomes the opportunity to share its experience promoting consumer privacy and data security with the FCC and looks forward to working with the FCC to ensure a consistent, efficient, and effective approach to enforcement and oversight in the broadband area."[22] At the same time, although the FCC has primary regulatory authority over telecommunications carriers, the FTC has not shied away from bringing actions against those carriers under certain circumstances for alleged unfair or deceptive business practices. For example, the FTC has taken action against a number of mobile carriers, alleging that they engaged in "cramming" – the illegal practice of subtly adding extraneous charges, typically from unauthorized third parties, into customers' telephone bills.

The FCC's Regulatory Authority To Protect Consumer Privacy

While the FCC's actions in the TerraCom and YourTel matter relied on sections 222(a) and 201(b) of the Communications Act, those actions should also be examined in the context of the FCC's other, more clearly delineated, authority to protect consumer privacy. Specifically, the FCC has authority under the Telecommunications Act of 1996, which amended the Communications Act, to regulate how telecommunications companies protect CPNI. Furthermore, the FCC has authority under the Telephone Consumer Protection Act ("TCPA") to regulate how all companies—not just telecommunications companies—utilize telecommunications systems to interact with customers (e.g. by making phone calls or sending faxes). Under both of these privacy protection regimes, the FCC's authority and the scope of the conduct prohibited is clearly laid out in statute and/or regulation—in notable contrast to the FCC's purported authority to regulate data security practices.

The Telecommunications Act of 1996, and the regulations promulgated pursuant to it, define what safeguards telecommunications companies must put in place to prevent the improper release of CPNI.[23] These safeguards include CPNI training requirements for employees and the implementation of supervisory review processes to ensure the security of CPNI. Other provisions dictate that telecommunications providers must obtain a customer's approval to use that customer's personal information in marketing activities; providers obtain this approval either by asking the customer to affirmatively "opt-in" to marketing use or by sending the customer a written notice about how the company intends to use the customer's information and giving the customer the ability to "opt-out." Recently, **the FCC brought an action against a major mobile carrier**, alleging that the company violated the FCC's CPNI regulations when it used call-related personal information from nearly two million subscribers to target them for advertising without their consent.[24] The FCC specifically alleged that the carrier failed to inform its customers of how to opt out of having their call-related personal information used in marketing campaigns. The FCC claimed that the carrier, despite becoming aware of the opt-out issue in September 2012, did not notify the agency of the issue until January 2013. In September 2014 the mobile carrier agreed to pay $7.4 million to settle the case, which at the time was the largest payment in a telephone customer privacy case.[25]

The TCPA prohibits the use of telephonic equipment in a variety of ways, and strictly regulates the use of automated telephone dialing systems, pre-recorded calls, and fax machines; the TCPA also grants the FCC the

authority to issue implementing regulations further defining what telecommunications activity is permissible.[26] For example, under the TCPA, it is unlawful for anyone to make any non-emergency call to a cellular telephone using an automated telephone dialing system without the prior express consent of the called party. The FCC has construed the statutory term "call" as including text messages.[27] For calls (or text messages) that are promotional in nature, the FCC requires *written* consent of the called party.[28] Companies that send promotional messages in this manner typically store the called party's written consent electronically together with other information about the call, such as the date and time.[29] This information must be stored in an electronic or other medium that is retrievable and in perceivable form.[30] Recently, Jiffy Lube International, Inc. settled a $47 million class action suit for allegedly sending a promotional text message to millions of consumers who had not consented to receive such text messages.[31] Additionally, a number of major financial institutions have recently settled TCPA class actions in amounts ranging from $32 million to $75.5 million for allegedly using automated dialers to call or text customers' cellphones without their consent.

Where Does This Issue Go From Here?

Although the FCC's CPNI regulations and the TCPA govern how companies *use* their customers' personal information, neither set of laws expressly grants the FCC the authority to regulate how telecommunications companies *secure or store* their customers' personal information; in other words, these laws do not expressly grant the FCC authority to regulate data security. As mentioned, the FCC claims that its authority for imposing the $10 million fine upon TerraCom and YourTel – and, implicitly, for regulating data security – is derived not from CPNI regulations or the TCPA, but from the Communications Act, which specifically states in section 222(a) that "[e]very telecommunications carrier has a *duty to protect* the confidentiality of *proprietary information* of, and relating to, other telecommunication carriers, equipment manufacturers, and customers . . . ."[32] According to the FCC, the Communications Act requires carriers to "take every reasonable precaution to protect the confidentiality" of their customers' information and the FCC must "take resolute enforcement action to ensure that the goals of [the Communications Act] are achieved."[33]

The FTC recently also has attempted to expand the scope of its authority to regulate data security; it has done so by broadening its definition of the phrase "unfair business practices" as used in the FTC Act. In a recent case, Wyndham Worldwide Corporation argued that the FTC cannot regulate corporate security practices because it has not published rules governing cybersecurity standards that would provide adequate notice to companies of the standards to which they are being held—which is precisely the point made by the dissenting FCC Commissioners in the TerraCom and YourTel cases. The FTC responded that Wyndham's security practices constituted "unfair" acts or practices because they caused or were likely to cause substantial injury to consumers that the consumers could not reasonably avoid themselves. The FCC may now be attempting to expand the scope of its authority in a similar manner: by broadening the definition of "duty to protect" and "proprietary information" in section 222(a) of the Communications Act.[34] In its order against TerraCom and YourTel, the FCC defines the "duty to protect" as a duty to protect customer personal information not just from misuse by the telecommunications carriers, but from misuse by *anyone* who obtains it from the carriers, even if they do so without the carriers' knowledge.[35] Furthermore, the FCC defines "proprietary information" as PII, rather than CPNI, greatly expanding the extent of information that telecommunications companies must protect.[36]

The FCC's recent actions pose a greater threat than those of the FTC to telecommunications carriers due to the FCC's ability to penalize a company immediately for a security defect. Generally, when the FTC determines that a business practice is "unfair," it issues a "cease and desist order" to the company before escalating the matter; if the company persists with the unfair practice, then the FTC may seek civil penalties from the company.[37] No such limitations exist for the FCC under the Communications Act; once a company has been convicted of failing to protect the "confidentiality of proprietary information of [its] customers," the FCC may impose a fine on the

company without further steps or notice.[38] The FCC here calculated the fine for violations of the Communications Act by using a base forfeiture of $29,000 per violation – and because the FCC counts each personal record that is unprotected as a distinct violation, its fines are likely to be significant.[39]

Conclusion

Regardless of whether any telecommunications companies challenge the FCC's enforcement of data security regulations as overly broad, telecommunications companies should expect continued scrutiny of their data security and other privacy practices, whether from the FCC or other regulators or authorities. That fact, along with the possibility of harsh FCC penalties, should encourage telecommunications companies to remain diligent in taking the steps necessary to reasonably protect all of their customers' personal information, whether PII, CPNI, or otherwise.

* * *

King & Spalding's Data, Privacy, and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigations, e-discovery / e-disclosure, government investigations, government advocacy, insurance recovery, and public policy.

---

[1] The authors would like to express their gratitude to Bethany Rupert and Jimmy Michaels, associates in King & Spalding's Special Matters / Government Investigations Practice Group, for their assistance with this Client Alert.
[2] *See* Press Release, Fed. Commc'ns Comm'n, *FCC Plans $10 Million Fine for Carriers that Breached Consumer Privacy* (Oct. 24, 2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db1024/DOC-330136A1.pdf.
[3] *See* Brian Fung, *With a $10 Million Fine, the FCC is Leaping Into Data Security for the First Time*, WASHINGTON POST (Oct. 24, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/24/with-a-10-million-fine-the-fcc-is-leaping-into-data-security-for-the-first-time/.

[4] Allison Grande, *FCC Wades Into Data Security with $10M Privacy Breach Fine*, LAW360 (Oct. 24, 2014), http://www.law360.com/privacy/articles/590260?nl_pk=2a377708-d285-4b6f-b687-d77c47c42d92&utm_source=newsletter&utm_medium=email&utm_campaign=privacy.
[5] *See id.*.
[6] *See id*.
[7] *See* Brian Fung, *supra* note 3.
[8] Press Release, *supra* note 2.
[9] Notice of Apparent Liability for Forfeiture, *In re: TerraCom, Inc. and YourTel Am., Inc.*, FCC 14-173 (Oct. 24, 2014) at 19. .
[10] *See* Allison Grande, *supra* note 4; Brian Fung, *supra* note 3.
[11] *See* Allison Grande, *supra* note 4.
[12] *See* 47 U.S.C. § 222(h)(1).
[13] Notice of Apparent Liability for Forfeiture,, *supra* note 9 at 7-8.
[14] *See id*.
[15] *Id*. at 27.
[16] *Id*. at 25.
[17] *Id*. at 26.
[18] *Id*.
[19] *See* Alden Abbott, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?* (The Heritage Found., Legal Memorandum #137 on Legal Issues, Sept. 10, 2014), *available at* http://www.heritage.org/research/reports/2014/09/the-federal-trade-commissions-role-in-online-security-data-protector-or-dictator#_ftn8. The FTC's Safeguards Rule, which it adopted pursuant to the Gramm–Leach–Bliley Act, requires non-bank financial institutions to develop and maintain comprehensive data security programs "to protect the security, confidentiality, and integrity of customer information." 16 C.F.R. § 314.1(a). The FCRA requires consumer reporting agencies to use reasonable precautions to ensure that they disclose sensitive consumer information only to permissible entities; the FCRA also obliges entities that maintain consumer report information to dispose of that information in a safe manner. *See* 15 U.S.C. § 1681e, 1681w. COPPA regulates the collection of personal information from children through a website or online service; specifically, the Act empowers the FTC to oversee website or online operators that collect personal information from children and to require that those operators obtain parental consent "for the collection, use, or disclosure of [that] information." 15 U.S.C. § 6502(b)(1)(A)(ii); *see* 15 U.S.C. §§ 6501–6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").
[20] *Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?*, Statement Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 109th Congress (Sept. 29, 2006) (prepared statement of the Fed. Trade Comm'n), available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-internet-data-brokers-and-pretexting/p065409internetdatabrokers09292006.pdf.
[21] *Id*. at 5 n.13 (citing the Telecommunications Act of 1996 "which amended the Communications Act, and accordingly [] afforded privacy protections [to consumer telephone records] by the regulations under that Act. See 42 U.S.C. § 222; 47 C.F.R. §§ 64.2001-64.2009.").
[22] Comment of the Fed. Trade Comm'n at 12, *In re: Inquiry Concerning the Deployment of Advanced Telecommunications Capability*, FCC GN Dkt. No. 14-126 (Sept. 22, 2014), *available at* http://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-federal-communications-commission-regarding-privacy-security/140919privacybroadband.pdf..
[23] *See* 47 U.S.C. § 222; 47 C.F.R § 64.2009.
[24] *See* David Siegel, *Verizon to Pay Record $7.4M to End FCC Privacy Probe*, Law360 (Sept. 3, 2014, 3:20 PM), http://www.law360.com/articles/573555.
[25] *See id.*
[26] *See* 47 U.S.C. § 227.
[27] *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 18 FCC Rcd. 14014, 14115 (2003).
[28] *See In re Rules and Regs. Implementing the Telephone Consumer Protection Act of 1991*, 27 F.C.C.R. 1830, 27 FCC Rcd. 1830, 1844 (Feb. 15 2012) ("2012 FCC Order").
[29] Presumably, telecommunications companies are required to protect the electronic records of these written consents either under the FCC's CPNI requirements or other FTC "business practice" requirements.
[30] 15 U.S.C. §7006 (4), (9).
[31] Lana Birbrair, *CORRECTED: Jiffy Lube Franchisee to Pay up to $47M to Settle Spam Text MDL*, Law360 (Aug. 2, 2012, 8:30 PM), http://www.law360.com/articles/366217/corrected-jiffy-lube-franchisee-to-pay-up-to-47m-to-settle-spam-text-mdl.

[32] 47 U.S.C. § 222(a) (emphasis added).
[33] Notice of Apparent Liability for Forfeiture, *supra* note 9 at 6, para. 13 & nn.30-31 (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959-60 (2007)), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db1027/FCC-14-173A1.pdf.
[34] *See* 47 U.S.C. § 222(a).
[35] *See* Notice of Apparent Liability for Forfeiture, *supra* note 9 at 11.
[36] *See id.*at 7-8, 10-11.
[37] Memo, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, Section II: Enforcement Authority (Fed. Trade Comm'n *Revised* July 2008), *available at* http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
[38] *See* 47 U.S.C. § 501.
[39] Notice of Apparent Liability for Forfeiture, *supra* note 9 at 19.