VENABLE LLP

the download

DEVELOPMENTS IN E-COMMERCE, PRIVACY, MARKETING AND INFORMATION SERVICES LAW AND POLICY

APRIL 2009

E-COMMERCE, PRIVACY, AND MARKETING ATTORNEYS

Two of the "Top 25 Privacy Experts" by *Computerworld* 2007

"Winning particular plaudits" for "sophisticated enforcement work"– *Chambers and Partners*

Recognized in the 2008 United States editions of *Chambers USA* and *Legal 500* for its outstanding data protection and privacy practice

ISSUE EDITORS

Stuart P. Ingis
singis@Venable.com
202.344.4613

Michael A. Signorelli
masignorelli@Venable.com
202.344.8050

ADDITIONAL CONTRIBUTORS

Emilio W. Cividanes
ecividanes@Venable.com
202.344.4414

Thomas A. Cohn
tacohn@Venable.com
212.370.6256

Ellen Traupman Berge
etberge@Venable.com
202.344.4704

Tara M. Sugiyama
tmsugiyama@Venable.com
202.344.4363

Julia Kernochan Tama
jktama@Venable.com
202.344.4878

1.888.VENABLE
www.Venable.com

In this Issue:

Around the Agencies:

- Law Enforcement Risks for Advertisers, Affiliates & Networks
- FTC Declares Identity Theft Red Flags Rule Applies to Health Care Professionals
- FTC Asserts Jurisdiction to Investigate Security of Personal Health Data

New Laws:

- Federal Stimulus Package Includes Dramatic Changes to Health Privacy and Security Law

In the Courts:

- NCTA v. FCC: The Use of Consumer Information for Marketing Purposes

From the States:

- Massachusetts Revises and Further Delays Implementation of New Data Security Regulations

As Congress moves through its legislative agenda, onward towards health care and financial regulatory reform, issues implicating privacy and data security are becoming more prevalent. For instance, in the recently-enacted stimulus law, policymakers considered the appropriate balance between protecting consumers' privacy interests in health information and the goal of establishing frameworks that foster efficient access to and legitimate uses of this data.

The coming months will likely include an increase in the introduction of privacy-related legislation. They will also include a renewed focus by the Federal Trade Commission on consumer protection issues. In March, President Obama designated Jon Leibowitz as the Chairman of the Federal Trade Commission. During a recent speech, the new Chairman expressed his commitment to protecting consumer privacy. Chairman Leibowitz has also stated that data security is a top priority, and has pledged that the Commission will enforce security requirements.

This issue of the *Download* includes a survey of recent agency actions, court decisions, new laws, and regulations that address collection, use, and accessing of consumer information. Included in this issue are articles on the application of the Red Flag Rules to health care providers, the Federal Trade Commission's

asserted jurisdiction over personal health data, a new law that adds significant privacy and security duties for entities that are already covered by the Health Insurance Portability and Accountability Act, and a court decision that recognizes consumers' privacy interests in controlling the use or disclosure of their information for marketing purposes. Also in this issue is an update on the Massachusetts data security regulations.

AROUND THE AGENCIES

Law Enforcement Risks for Advertisers, Affiliates & Networks

I. FTC Principles For Online Negative Option Marketing

On February 9, the Federal Trade Commission ("FTC") issued a staff report summarizing its Negative Option workshop held two years ago and the comments it received. FTC staff defined "negative option marketing" broadly as a "category of commercial transactions in which sellers interpret a customer's failure to take an affirmative action, either to reject an offer or cancel an agreement, as assent to be charged for goods or services." Negative option marketing can take a variety of forms, including free trial offers, continuity plans, membership clubs, automatic subscription renewals, and pre-notification plans.

FTC staff identified the following five principles to guide online marketers of negative option offers in complying with Section 5 of the FTC Act when making such offers:[1]

1. **Marketers should disclose the offer's material terms in an understandable manner.** The material terms of negative option offers include: the existence of the offer, the offer's total cost, the transfer of a consumer's billing information to a third party (if applicable), and how to cancel the offer. Marketers should avoid making disclosures that are vague, unnecessarily long, or contain contradictory language.

2. **Marketers should make the appearance of disclosures clear and conspicuous.** To make online negative option disclosures clear and conspicuous marketers should place them in locations on web pages where they are likely to be seen, label the disclosures (and any links to them) to indicate the importance and relevance of the information, and use text that is easy to read on the screen.

3. **Marketers should disclose the offer's material terms before consumers pay or incur a financial obligation.** Marketers should disclose an offer's material terms before consumers agree to purchase the item. Consumers often agree to an offer by clicking a "submit" button; therefore, disclosures should appear before consumers click that button.

4. **Marketers should obtain consumers' affirmative consent to the offer.** Marketers should require that consumers take an affirmative step to demonstrate consent to an online negative option offer. Marketers should not rely on a pre-checked box as evidence of consent. However, clicking a button such as "I agree" is a sufficient affirmative step to demonstrate consent, provided disclosures are made as described above.

[1] *See* Federal Trade Commission Report, *A Report by the Staff of the FTC's Division of Enforcement: Negative Options,* January 2009, available at http://www.ftc.gov/os/2009/02/P064202negativeoptionreport.pdf.

5. **Marketers should not impede the effective operation of promised cancellation procedures.** Marketers should employ cancellation procedures that allow consumers to effectively cancel negative option plans. Marketers should not engage in practices that make cancellation burdensome for consumers, such as requiring consumers to wait on hold for unreasonably long periods of time.

These principles do not have the force of law and are intended merely to guide industry in complying with Section 5 of the FTC Act. However, online marketers of negative option offers should take careful note of these new FTC principles, as noncompliance may draw the attention of FTC staff and be the basis for an investigation and/or law enforcement action. If the FTC does take action, it may seek order provisions more stringent than what the principles recommend. At the same time the FTC issued this report, it announced two consent orders concerning allegedly deceptive online negative option offers.[2] These orders enjoined defendants from misrepresenting:

> that a product or service is offered on a "free," "trial," or "no obligation" basis, or words of similar import, denoting or implying the absence of any obligation on the part of the recipient of the offer to affirmatively act in order to avoid charges if, in fact, a charge will be assessed pursuant to the offer unless the consumer takes affirmative action to cancel.[3]

II. Consumer Blogs, Celebrity/Expert Endorsements, Product Claims

Negative option offers have also triggered law enforcement scrutiny of the advertising claims for the particular products being sold, and the substantiation for those claims. Several state attorneys general have recently stepped up their investigations and enforcement actions concerning the online marketing of various dietary supplements, citing these very issues. The state attorneys general have alleged a wide variety of questionable practices, from false and/or unsubstantiated product claims, to deceptive trial offers with improper or unauthorized charges, to falsely implied celebrity/expert endorsements, and fake consumer blogs.

Affiliate-created blogs, review sites and other web pages have proliferated in recent years, and have been filled with product claims, reviews, endorsements, and testimonials that increasingly drive consumer traffic to online sellers of dietary supplements and other products. When such web pages contain false or unsubstantiated claims (express or implied), or fail to disclose material connections with sellers, there is the possibility of affiliate and/or network liability, for deceptively driving online sales of such products.

The FTC has consistently stated that parties other than the advertiser may be liable for deceptive advertising if they played a role in the promotion. In fact, the FTC takes the position that a party may be responsible for any ad claims it makes that may be passed downstream to others: "It is [a] well settled law that the originator is liable if it passes on a false or misleading representation with knowledge or reason to expect that consumers may possibly be deceived as a result."[4]

---

[2] *See* FTC Press Release, *FTC Targets Weight-Loss Marketers' Allegedly Bogus 'Free' Sample Offers*, February 9, 2009, available at http://www.ftc.gov/opa/2009/02/jab.shtm.

[3] *FTC v. JAB VENTURES, LLC*, Stipulated Final Order for Permanent Injunction and Other Equitable Relief, Civil No. CV08-4648-SVW(RZx), (August 20, 2008), available at http://www.ftc.gov/os/caselist/0623109/090209jaborder.pdf.

[4] Statement of FTC Chairman Pitofsky and Commissioners Anthony and Thompson, *In re Shell Oil Company* (1999).

In fact, the FTC has held ad agencies, endorsers, and shopping channels liable for their roles in allegedly false or deceptive advertising. Could these same principles be applied to affiliate marketers and/or advertising networks who create or approve such traffic-driving techniques as false endorsements, phony reviews or fake blogs? Yes, but neither the FTC nor any state attorney general has directly confronted this issue – yet. The FTC, though, has proposed revisions to its Endorsements and Testimonials Guides, making clear that both advertisers and new media that promote advertised products (such as online reviews and blogs) could be held liable for false advertising claims appearing in these new media contexts, as well as for failing to disclose material connections between advertisers and these new media promoters.

III. The Perfect Storm?

Given these FTC's positions, it is possible that, beyond online sellers' own advertising liability, affiliate marketers and/or advertising networks could be held liable for the consumer injury allegedly resulting from practices such as fake blogs, falsely implied celebrity/expert endorsements, and failures to disclose compensation from advertisers, all of which increase consumer traffic to the sellers' landing pages. In fact, there is now a heightened risk that this "perfect storm" of marketing practices, product claims, and affiliate marketing techniques could be challenged, singly or in any combination, by the state attorneys general and/or the FTC. Therefore, anyone in the advertising stream with the requisite knowledge might end up in the crosshairs of law enforcement: advertiser, affiliate, and/or network.

Careful attention now to the drafting of online offers and affiliate web pages, together with the advice of counsel having relevant experience, may help advertisers, affiliates and ad networks to avoid unwanted law enforcement scrutiny down the road, and to develop the proper responses should this happen.

FTC Declares Identity Theft Red Flags Rule Applies to Health Care Professionals

Federal Trade Commission ("FTC" or the "Commission") Acting Director of the Bureau of Consumer Protection Eileen Harrington issued a letter on February 4, 2009 (the "FTC-AMA Letter") stating that the Identity Theft Red Flags Rule ("Red Flags Rule" or the "Rule") applies to physicians and related health care providers when they regularly defer payment for goods or services. Over the last several months, the American Medical Association ("AMA") and the FTC have clashed over whether the Red Flags Rule covers health care professionals, with the former taking the position that such professionals are not creditors covered by the Rule and the latter asserting that the Rule encompasses such health care providers. While the debate continues, in light of the FTC-AMA Letter and the fast-approaching May 1, 2009 effective date of the Rule, health care providers should consider whether they have procedures in place to comply with the Red Flags Rule.

I. The Red Flags Rule

The Red Flags Rule requires covered entities, including creditors and financial institutions, to develop and implement identity theft programs designed to identify, detect, and respond to possible risks of identity theft. The Rule was developed in response to a mandate in the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended the Fair Credit Reporting Act ("FCRA"). Financial institutions and creditors were originally given until November 1, 2008

to comply with the Rule, but in October 2008, the FTC extended the compliance deadline for creditors until May 1, 2009. During this time, the AMA has maintained the position that the Red Flags Rule does not cover physicians and related health care providers. The FTC-AMA Letter challenges this interpretation of the Rule.

II. The FTC-AMA Letter

The FTC-AMA Letter asserts that the plain language and purpose of the Red Flags Rule necessitate that the Rule apply to physicians and related health care providers when they regularly defer payment for services. The FTC-AMA Letter reaches this conclusion that medical practitioners constitute "creditors" covered by the Red Flags Rule after conducting a review of the terms "creditor" and "credit" as they are defined in the Rule, and consulting the Official Staff Commentary to Regulation B, the Fair Credit Reporting Medical Information Regulations, and select court cases. The FTC-AMA Letter explains that according to these sources, the term "creditor" should be interpreted broadly to include health care providers who permit the deferment of payment for their medical services.

III. Complying with the Red Flags Rule

The FTC-AMA Letter notes that the burden on health care professionals need not be substantial to comply with the Red Flags Rule and further the purpose of the Rule to reduce incidents of identity theft, including medical identity theft. The FTC-AMA Letter explains that the Rule is risk-based and, accordingly, that the identity theft programs that covered entities develop need only be commensurate with the risk that they face. For example, for physicians in a low risk setting, the FTC-AMA Letter suggests that an appropriate program would include requiring a patient's photo identification to be checked at the time the patient seeks services. The letter also explains that such a program should have procedures in place to respond if the physician learns that a patient's identity has been misused, such as: (1) avoiding collecting the debt from the true patient or (2) refraining from reporting the debt on the true patient's credit report, and (3) ensuring medical information about the identity thief is separated from the true patient. The FTC-AMA Letter further explains that compliance with both the Red Flags Rule and HIPAA is necessary to implement a comprehensive approach to combat medical identity theft.

FTC Asserts Jurisdiction to Investigate Security of Personal Health Data

On February 18, 2009, the Federal Trade Commission ("FTC") and the Office for Civil Rights in the Department of Health and Human Services ("HHS") reached coordinated consent agreements with CVS Caremark ("CVS") on charges that CVS did not adequately secure the sensitive information of its customers and employees. The CVS case is notable for the FTC's energetic pursuit of an enforcement action involving personal health data. When CVS challenged the FTC's jurisdiction, the FTC rejected CVS's argument that HHS has exclusive authority to enforce the privacy of protected health information ("PHI").

HHS and the FTC launched their joint investigation in the wake of media reports that CVS pharmacies had discarded materials with readable personal information, such as employee records and prescriptions, in unsecured public dumpsters. The FTC advised CVS of its inquiry in September 2007. On May 22, 2008, CVS received a Civil Investigative Demand ("CID") from the FTC seeking additional documents and information. CVS petitioned to quash or limit the CID, arguing that

the demand was unreasonable and that the FTC lacked jurisdiction to enforce the privacy and security of PHI that is already regulated by HHS pursuant to the Health Insurance Portability and Accountability Act ("HIPAA").

On August 6, 2008, Commissioner Pamela Jones Harbour denied CVS's petition. Commissioner Harbour stated that CVS had failed to support its claims that HHS has exclusive jurisdiction over PHI protection matters, or that HIPAA precluded the FTC from addressing such matters. Commissioner Harbour noted that the investigation was a coordinated effort of the two agencies, and contended that agency jurisdiction should not be trammeled during the early stages of an investigation. The FTC reviewed Commissioner Harbour's ruling at CVS's request, and affirmed it on December 3, 2008. The FTC agreed with Commissioner Harbour that CVS had failed to support its contention that the FTC lacked jurisdiction, and also noted that the data involved in the publicized incidents was not limited to health information.

The FTC alleged in its complaint that CVS routinely collected sensitive personal information from customers, including prescription information and Social Security account numbers, and that CVS also collected Social Security account numbers and other personal information from employees. In its complaint, the FTC contended that CVS engaged in an unfair trade act or practice by failing to: (1) implement data security policies and procedures, (2) train employees, (3) assess compliance, or (4) establish a process for discovering and remedying security risks. The FTC further argued that, in light of these alleged failures, the CVS privacy policy was false or misleading.

The proposed FTC consent agreement applies to prescription information as well as other individual data. The agreement states that CVS must establish a comprehensive data security program to safeguard the personal information of customers and employees. Among other features, the program must include a thorough risk assessment and the adoption of "reasonable steps" to ensure that CVS's outside contractors also follow sound data security practices. To verify compliance, CVS is required to submit to an independent security audit every two years for the next 20 years and to maintain compliance records for FTC inspection for three to five years.

HHS alleged that CVS violated the Health Insurance Portability and Accountability Act Privacy Rule by failing to establish procedures on proper disposal of protected health information ("PHI"), to train employees, or to punish non-complying employees. The settlement requires CVS to pay $2.25 million in restitution and implement a corrective action plan. Under this plan, CVS will create and adopt new disposal policies for PHI, train employees in the policies, sanction employees who do not comply, and set up internal mechanisms so that employees can report privacy violations. CVS must also provide HHS with compliance reports for the next three years.

NEW LAWS

Federal Stimulus Package Includes Dramatic Changes to Health Privacy and Security Law

The Health Information Technology for Economic and Clinical Health ("HITECH") Act became law on February 17, 2009, as Title XIII of the American Recovery and Reinvestment Act of 2009 ("ARRA"). The HITECH Act sets the stage for a national transition to electronic health records, while other sections of ARRA provide about $19 billion in funding to encourage this transition. At the same time, the HITECH

Act adds significant new privacy and security duties for entities that are already covered by the Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules, including a requirement to notify patients whose data is compromised by a security breach. The legislation also applies HIPAA security requirements to business associates of covered entities, tightens limits on health marketing communications, and introduces a data breach notification rule for health records vendors and certain marketers.

I. On the Horizon: New Rulemakings by the Secretary of Health and Human Services and the Federal Trade Commission

Going forward, the HITECH Act directs federal agencies to issue additional regulations and reports that will continue to define companies' obligations and shape the health privacy landscape for the next several years. Specifically:

- Within six months, HHS must issue guidance to define when protected health information ("PHI") is "unsecured" such that a data breach requires patient notification, and must issue interim final regulations to implement the new data breach notification rule for covered entities and business associates.

- Also within six months, the Federal Trade Commission (FTC) must issue regulations implementing a breach notification rule for vendors of personal health records, online marketers on health websites, and other users of electronic health records. The notification requirements will take effect 30 days after these regulations come out. FTC issued its notice of proposed rulemaking and request for public comment on April 16, 2009. Comments are due June 1, 2009.

- Within one year, HHS must report to Congress on whether HIPAA privacy and security rules should apply to vendors of personal health records, online marketers on health websites, and other users of electronic health records.

- Within 18 months, the Secretary of Health and Human Services (HHS) must issue regulations governing paid disclosures and marketing uses of PHI, which will take effect six months thereafter.

Although the forthcoming HHS and FTC rulemakings on data breach notification will be limited to health data, the final regulations are likely to influence debate on any broader notification bill that is taken up by the 111th Congress. Such bills have already been introduced, and proponents may be emboldened to push for their consideration following the inclusion of breach notification provisions in the HITECH Act.

II. Significant Provisions of the HITECH Act

The HITECH Act includes the following major changes to prior law and policy:

Extends HIPAA rules to business associates of health care providers: Previously, HIPAA rules applied only to certain "covered entities," such as hospitals and physicians, which were required to write contracts holding their business associates to the same rules. Under the HITECH Act, business associates are directly required to adopt HIPAA-compliant administrative, physical and technical safeguards for electronic PHI, and will be exposed to civil and criminal penalties for failures to comply.

Imposes new health data breach notification requirements: Covered entities are required to promptly notify any patients whose unsecured PHI is affected by a security breach, other than a mistaken, in-house unauthorized access. If the

breach affects more than 500 people, the covered entity must also notify HHS and media outlets. In turn, business associates must notify covered entities. The HITECH Act also requires breach notification to affected individuals and the FTC by vendors of personal health records, marketers that advertise on the websites of vendors or covered entities, and others who access electronic health records.

Tightens limits on marketing uses and disclosures of PHI in exchange for payment: Previously, covered entities were allowed to accept payment from third parties in exchange for sending marketing communications to patients, because these communications could be considered "health care operations." The HITECH Act states that paid communications cannot be health care operations, with the narrow exception that covered entities may still receive reasonable payment for communications about drugs or biologics for which patients have a current prescription. The HITECH Act also tightens PHI disclosure rules by barring covered entities and business associates from directly or indirectly selling a patient's PHI to a third party without the patient's specific consent. There is a limited set of exceptions to this rule, such as sales for public health or research purposes.

Refines existing rules about how PHI is shared and handled: The HITECH Act gives patients additional rights to restrict disclosures of their PHI and to obtain information about how their PHI is disclosed. The Act also requires the Secretary of Health and Human Services to issue guidance clarifying an existing regulation that limits disclosures of PHI to the minimum information necessary to fulfill a request.

Expands enforcement mechanisms and penalties: The HITECH Act increases civil penalties for violations of privacy and security rules, extends civil and criminal penalties to business associates, and directs the Secretary of Health and Human Services to penalize covered entities and business associates that willfully neglect to comply with privacy and security rules. The legislation also empowers state attorneys general to investigate and pursue violations of the law as long as no federal action is pending.

IN THE COURTS

NCTA v. FCC: The Use of Consumer Information for Marketing Purposes

On February 13, 2009, the DC Circuit Court of Appeals upheld the Federal Communications Commission's 2007 Order that requires telecommunications carriers to obtain a customer's prior affirmative consent before disclosing customer proprietary network information ("CPNI") to joint ventures and independent contractors for the purpose of marketing communications-related services to that customer.[5] The Court found the Federal Communications Commission's ("Commission" or "FCC") decision to impose an opt-in scheme constitutional.[6] Previously, disclosures of a customer's CPNI by telecommunications carriers to joint ventures and independent contractors were prohibited if the customer opted out of the carrier's use or disclosure of CPNI. In addition to upholding the Commission order, the Court's decision broadly recognizes a consumers' privacy interests in controlling the use or disclosure of their information for marketing purposes.

[5] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C.R. 6927 (2007) (hereinafter 2007 Order).

[6] *National Cable & Telecommunications Assoc. v. Federal Communications Commission*, 2009 U.S. App. LEXIS 2828 (D.C. Cir. Feb 13, 2009).

I. Background

Telecommunications carriers are required by law to "protect the confidentiality of proprietary information of…customers."[7] This proprietary information, known as CPNI, consists of call detail information, which is information relating to who a customer calls, for how long, and when, and the kinds of services (i.e. calling plans) and features (i.e. call waiting) the customer purchases from their carrier. Carriers often use this information to market specific services to their customers. The Telecommunications Act, however, prohibits a carrier from using, disclosing, or allowing access to CPNI without the approval of the consumer. Prior to the 2007 Order, the Commission maintained a rule that "customer approval" meant a request by the customer that the carrier not use, disclose, or allow access to their CPNI. Through the 2007 Order, the Commission adopted an "opt-in" scheme.

II. Regulation of CPNI Prior to the 2007 Order

In 1998, the Commission released an order that required carriers to obtain prior affirmative and explicit consent for certain uses of CPNI, but recognized that for other certain data uses, carriers could infer consent.[8] Whether a carrier was required to obtain a customer's "opt-in" consent or provide the opportunity to "opt-out" depended on whether the use of data was related to an existing service. If a proposed data use or disclosure was outside of an existing relationship between the carrier and customer, the carrier was required to obtain the customer's "opt-in" consent. This rule implicated data sharing between a carrier and its affiliates. The 1998 order was challenged in the courts (*U.S. West v. FCC*) and found to be an unconstitutional restriction on a carrier's First Amendment right to speak to its customers.[9] Following *U.S. West*, the Commission issued a new order that required only opt-out approval for sharing of CPNI between carriers and its affiliates.[10] The Commission also permitted carriers to share CPNI with joint ventures and independent contractors for marketing communications-related purposes if the parties entered confidentiality agreements to safeguard the data.

III. The Commission's 2007 Order

In 2005, the Commission was petitioned to commence a rulemaking to modify the CPNI rules related to sharing information with joint ventures and independent contractors. The petitioner claimed that inadequate privacy protections have contributed to the rise in the number of pretexting incidents. In 2007, the Commission issued a new rule, which required carriers to "obtain opt-in consent from [the] customer before disclosing that customer's [CPNI] to a carrier's joint venture partner or independent contractor for the purpose of marketing communications-related services to that customer."[11] The order distinguished affiliates from joint ventures and independent contractors. The Commission stated that the information shared with joint ventures and independent contractors is subject to a greater risk of loss and that these types of entities would not likely be subject to the confidentiality requirements of 47 U.S.C. § 222.

---

[7] 47 U.S.C. § 222.

[8] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 13 F.C.C.R. 9061 (1998).

[9] *U.S. West v. FCC* 182 F.3d 1224 (10th Cir. 1999).

[10] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 17 F.C.C.R. 14860 (2002).

[11] 2007 Order, at ¶37.

IV. Court Challenge

The National Cable & Telecommunications Association ("NCTA") challenged the 2007 Order asserting that it violated the First Amendment to the Constitution or, alternatively, that it is arbitrary in violation of the Administrative Procedure Act. As in *U.S. West*, the Court considered whether the Commission's rule is a permissible regulation of commercial speech. In doing so, the Court applied the following standards set forth in *Central Hudson Gas & Electric Corp v. Public Service Commission of New York*, 447 U.S. 557, 566 (1980): (1) the speech must "at least concern lawful activity and not be misleading;" (2) the "governmental interests [must be] substantial;" (3) the regulation must "directly advance[] the governmental interest asserted;" and (4) the regulation must not be "more extensive than is necessary to serve that interest."

The Court found the first prong of the *Central Hudson* test not at play. With regard to the second prong, the Court held that because NCTA did not challenge the constitutionality of 47 U.S.C. § 222, NCTA had conceded that there is a "substantial [government] interest in protecting the privacy of consumer information and that requiring customer approval advances that interest."[12] Notwithstanding this finding, the Court did discuss the government's substantial interest. Unlike the *U.S. West* court, which doubted whether protecting against the disclosure of CPNI could ever be deemed substantial, this court did find protecting the privacy of consumer information to be a substantial interest.[13] The Court further found that the interest in protecting consumer privacy involves more than preventing embarrassment, and "that privacy deals with determining for oneself when, how and to whom personal information will be disclosed to others."[14]

The Court then considered the third prong – whether the regulation "directly advances" the government interest. Again, because NCTA did not make a challenge to 47 U.S.C. § 222, NCTA conceded that the restriction Congress imposed—customer approval—was constitutional. The Court concluded that the Commission reasonably found "that an opt-in consent requirement directly and materially advances the interests in protecting customer privacy and in ensuring customer control over information."[15] The Court stated that it is "common sense" that the "risk of unauthorized disclosure of customer information increases with the number of entities possessing it."[16] Furthermore, the Court found that focusing on the information in the possession of joint ventures or independent contractors diverts attention from the fact that sharing the information "without the customer's consent is itself an invasion of the customer's privacy."[17]

The Court found that the Commission's adoption of opt-in consent satisfies the fourth prong – regulation must not be "more extensive than is necessary to serve that interest." The Court stated that opt-in consent, which assumes customers do not want their information shared with third-party marketers unless they expressly give consent, is an appropriate approach because evidence shows that customers are "less willing to have their information shared with third parties as opposed to affiliated entities."[18] The Court found that the adoption of an opt-in scheme is further supported by the "greater risk of disclosure once [information is] out of the control of the carriers and in the hands of entities not subject to [47 U.S.C.] § 222."[19] The Court stated that contractual safeguards (i.e. termination of a third-party contractor after a data breach) do not sufficiently protect consumer privacy because these remedies are effective after the consumer has been damaged.

---

[12] *National Cable & Telecommunications Assoc*, 2009 U.S. App. LEXIS at *12
[13] *Compare U.S. West, 182 F.3d at 1235 with National Cable & Telecommunications Assoc*, 2009 U.S. App. LEXIS at *12.
[14] *National Cable & Telecommunications Assoc*, 2009 U.S. App. LEXIS at *14.
[15] *Id.* at *16.
[16] *Id.*
[17] *Id.*
[18] *Id. at* *18.
[19] *Id.*

Finally, the Court denied the NCTA clam under the Administrative Procedure Act. The Court found that substantial evidence supported the Commission's order.

FROM THE STATES

Massachusetts Revises and Further Delays Implementation of New Data Security Regulations

The Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") has once again extended the implementation deadline for the identity theft prevention regulations designated in 201 Mass. Code Regs. 17.00 *et seq*. As we previously reported in the October and November/December 2008 issues of the Download, Massachusetts has taken measures to implement regulations establishing standards for how businesses must protect and store personal information of Massachusetts consumers. The regulations require the encryption of personal information stored on laptops and portable devices or transmitted across public networks or wirelessly. Originally scheduled to take effect on January 1, 2009, OCABR introduced a tiered deadline schedule on November 14, 2008 to provide businesses with additional time to comply with the regulations.

Citing a sharp change in the business climate and the goal of reducing administrative burdens on business, OCABR on February 12, 2009 announced a revision to the regulations and an additional delay in the implementation date. The newly revised regulations are now set to take effect on January 1, 2010.

In addition to delaying the compliance date, OCABR made a substantive change to its regulations. The original regulations would have required businesses to provide a written certification that their third-party vendors comply with the data security regulations. The revised regulations no longer require such written certification from third-party providers.

About Venable

One of *American Lawyer*'s top 100 law firms, Venable LLP has attorneys practicing in all areas of corporate and business law, complex litigation, intellectual property and government affairs. Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world from its headquarters in Washington, D.C. and offices in California, Maryland, New York, and Virginia.

Venable office locations

BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
25TH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

ROCKVILLE, MD
ONE CHURCH STREET
FIFTH FLOOR
ROCKVILLE, MD 20850
t 301.217.5600
f 301.217.5617

TOWSON, MD
210 ALLEGHENY AVENUE
TOWSON, MD 21204
t 410.494.6200
f 410.821.0147

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
t 703.760.1600
f 703.821.8949

WASHINGTON, DC
575 7TH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300