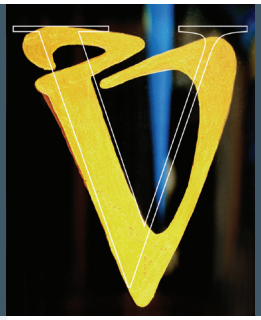
VENABLE LLP



the download

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

FEBRUARY 2009

E-COMMERCE, PRIVACY, AND MARKETING ATTORNEYS

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

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

Authors/editors of the forthcoming *BNA Portfolio on Privacy Law*

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

"Among the nation's first privacy lawyers"– *Chambers and Partners*

EDITORS AND CONTRIBUTORS

Emilio W. Cividanes
ecividanes@Venable.com
202.344.4414

Stuart P. Ingis
singis@Venable.com
202.344.4613

Michael A. Signorelli
masignorelli@Venable.com
202.344.8050

Tara M. Sugiyama
tmsugiyama@Venable.com
202.344.4363

Megan Malone
mmalone@Venable.com
202.344.4621

1.888.VENABLE
www.Venable.com

In this Issue:

2009 brings a new President, Congressional session, and a legislative and regulatory agenda. The focus thus far has been on the stimulus legislation. Quickly, however, the legislative priorities are will begin to take shape. Tied to the stimulus bill, health information technology and the privacy implications associated with the transfer and availability of the health related data has been an early focus of Congress. The coming year should be interesting as the Congress, with a Democratic majority, reveals its full agenda.

In this issue of the Download, there are articles on the Federal Trade Commission Staff's report on self-regulatory principles for online behavioral advertising, the Federal Trade Commission's announcement regarding an upcoming conference on data security, the Congressional hearings on health information technology, and a review of the new Administration's commitment to addressing cybersecurity. This issue also includes articles

on the US Supreme Court's decision to decline to review a ruling on the Child Online Protection Act and a summary of a New York Assembly bill that targets online advertising. Finally, there is an article that includes tips for complying with the US Safe Harbor program.

I. AROUND THE AGENCIES

FTC Staff Issue Report on Self-Regulatory Principles for Online Behavioral Advertising

On February 12, 2009, the Federal Trade Commission ("FTC" or "Commission") released the staff's final report on self-regulatory principles for online behavioral advertising.[1] Commission staff indicated that they sought to strike a balance with privacy concerns raised by the practice of online behavioral advertising with its benefits when developing the principle, which were originally proposed and opened for public comment on December 20, 2007. In the report, the FTC staff express their hope the principles will further encourage the development of meaningful self-regulatory principles that include meaningful enforcement mechanisms. The report also states that the staff intends to continue its inquiry into behavioral advertising. Timed with the release of the report, Commissioners Jon Leibowitz and Pamela Jones Harbour issued concurring statements, with Commissioner Leibowitz suggesting that more rigorous self-regulation was required to avoid legislation, and Commissioner Harbour calling on the FTC to conduct a broader examination of behavioral advertising within the privacy context.

The scope of the principles covers "online behavioral advertising," a term meaning "the tracking of a consumer's online activities over time – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individuals consumer's interests."[2] As a modification from the earlier proposal, the definition now clarifies that this definition is not intended to include "first party" advertising, where data is not shared with third parties, or contextual advertising, where ads are based on a single visit to a web page or single search query. The report also states that the principles cover any data collected for online behavioral advertising that "reasonably could be associated" with an consumer or device.[3]

Self-regulatory principles outlined in the report include: (1) transparency and consumer control; (2) reasonable security and limited data retention for consumer data; (3) affirmative express consent for material changes to existing privacy promises; and (4) affirmative express consent to or prohibition against using sensitive data for behavioral advertising.

A. Transparency and Consumer Control

The principle on transparency and consumer control states that every website that collects data for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement. According to the report, this statement should inform consumers that data is being collected on the site for use in providing them with advertising about products and services tailored to their interests, and that consumers have a choice about whether their information is collected for behavioral advertising. The report

also provides that websites should provide consumers with an easy-to-use and accessible method of exercising the option of whether their information is collected for such a purpose. Additionally, the report now states that companies should develop alternative methods outside the traditional website context to ensure disclosure and consumer choice when collecting data.

B. Reasonable Security and Limited Data Retention for Consumer Data

The principle on security and data retention states that any company collecting or storing consumer data for behavioral advertising should provide reasonable security. As previously proposed, the report indicates that such security should be based on the sensitivity of the data, nature of a company's business operations, risks a company faces, and reasonable available protections. Regarding data retention, the report now indicates that a company should retain data only as long as necessary for legitimate business purposes or law enforcement needs.

C. Affirmative Express Consent for Material Changes to Existing Privacy Promises

The principle on affirmative express consent for material changes to existing privacy promises provides that a company must maintain its promises pertaining to consumer data even if the company later changes its policies. Clarifying from the proposed principle, the new principle states that affirmative express consent should be acquired from consumers before using previously collected data in a manner materially different from the promises made.

D. Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising

The principle on affirmative express consent to or prohibition against using sensitive data for behavioral advertising states that a company may collect sensitive data only after obtaining affirmative express consent from the consumer. Staff expressed support for developing standards that define the term sensitive data.

FTC Announces Conference on Global Data Security Concerns

The Federal Trade Commission ("FTC") announced that it will host a two-day international conference to consider the data practices of companies. The FTC will co-host the conference with the Asia-Pacific Economic Cooperation forum and the Organisation for Economic Co-operation and Development. The conference, titled "Securing Personal Data in the Global Economy," will focus on data security issues in global information environments and will bring together public officials, technology experts, consumer advocates, academics, and industry representatives. The conference will be held in Washington, DC on March 16th through 17th, 2009.

The agenda for the conference will include six sessions covering a wide array of topics. One session will broadly identify data security issues implicated by the transfer of data among different legal jurisdictions. Another session will address the conflicts of law issues associated with multi-jurisdiction transfers while a different session will discuss whether certain data, such

as sensitive information, should be subject to a heightened level of security. Other panels will review the different data security legal regimes and discuss whether a single international standard could be created that protects consumers without unduly hindering the global information economy. Finally, another panel will examine current industry data security practices with an emphasis on data breach response practices.

Cybersecurity Is a Top Priority for President Obama and Congress

President Obama and Congress have tagged investment in cybersecurity as a means to help stimulate the economy. The stimulus bill, (H.R.1) passed by the House included $50 million for cybersecurity under the Public Health and Social Services Fund. The Senate's version has included an additional $14 million to fund enhanced cybersecurity research. Additionally, the Obama administration and Department of Homeland Security (DHS) have included cybersecurity as a focus in protecting the country's information networks.

According to the White House's Homeland Security Agenda, President Obama plans on appointing a national cyber advisor who will be responsible for coordinating federal agency efforts and development of national cyber policy. The Administration plans to work with the private sector to develop systems and technology to enhance the security of the nation's, current and future, computer hardware and software, storage and networks by implementing the following:

- *Initiate a Safe Computing R&D Effort and Harden our Nation's Cyber Infrastructure:* An initiative to develop next-generation secure computers and networking for national security applications. Work with industry and academia to develop and deploy a new generation of secure hardware and software for our critical cyber infrastructure.

- *Protect the IT Infrastructure That Keeps America's Economy Safe:* Work with the private sector to establish tough new standards for cybersecurity and physical resilience.

- *Prevent Corporate Cyber-Espionage:* Work with industry to develop the systems necessary to protect our nation's trade secrets and our research and development.

- *Develop a Cyber Crime Strategy to Minimize the Opportunities for Criminal Profit:* Eliminate mechanisms used to transmit criminal profits by shutting down untraceable Internet payment schemes. Initiate a grant and training program to provide federal, state, and local law enforcement agencies the tools they need to detect and prosecute cyber crime.

- *Mandate Standards for Securing Personal Data and Require Companies to Disclose Personal Information Data Breaches:* Partner with industry and our citizens to secure personal data stored on government and private systems. Institute a common standard for securing such data across industries and protect the rights of individuals in the information age.

On the regulatory side, the nominee for Secretary of DHS, Janet Napolitano, made cybersecurity a point of emphasis in her confirmation testimony. As a nominee, she indicated that she intends to take a close look at the Department's role in this area, working with the White House, other federal agencies, state governments and the private sector. Upon a swift confirmation by the Senate on January 20th, Secretary Napolitano, within the first week on the job, issued new action directives – one of which was cybersecurity. Each directive instructs specific agencies to gather information, review existing strategies and programs and to provide reports back to the Secretary. The agencies that the cybersecurity directive is focused on are the Departments of Defense, Treasury, and Energy, and the National Security Agency. A final report is due February 17th. Secretary Napolitano believes the directives "will unify our shared efforts and help me assess where improvements need to be made."

II. HEARD ON THE HILL

Congress Considers Health Information Technology

Congress is considering how health information technology ("HIT") could enhance the quality of healthcare as well as the privacy issues implicated with the use and transfer of electronic health records. In particular, Congress is considering how to leverage technology to increase the availability of healthcare, reduce costs, and improve access to medical records. During a recent hearing, Sen. Kennedy (D-MA) indicated through a prepared statement that "the health care industry continues to lag behind in implementing information technology, even though the potential for major improvement has been known for years."[4] He suggested that federal grants could spur investment in technology by the healthcare industry. In addition to improving healthcare, Congress is considering how investment in HIT could stimulate the economy. The proposed stimulus bill, H.R. 1, American Recovery and Reinvestment Act, would appropriate billions for investment into HIT technologies and for acquisition of HIT equipment by healthcare providers.

Two Senate committees held hearings in January 2009 to consider how HIT could improve the quality of healthcare and reduce healthcare expenses. The committees also considered the privacy issues implicated by HIT. Below is a summary of the key issues from those hearings.

A. The Senate Committee on Health, Education, Labor, and Pensions Working Group Quality Healthcare ("Working Group")

The Working Group held a hearing on January 15th to consider how technology could improve the quality of healthcare and reduce inefficiencies and expenses in the national healthcare system. Through a prepared statement, Sen. Kennedy (D-MA) recognized HIT's value to the healthcare system and indicated that HIT could be used to reduce errors, revolutionize treatment, and increase access to quality healthcare at lower costs. Other members weighed in on the issue during the hearing. Sen. Mikulski (D-MD) stated that the government would rely on the private sector to help develop and implement HIT. Sen. Merkley (D-OR) inquired into the kinds of efforts necessary to bring HIT to rural communities and the type of patient data that could be made available to healthcare providers should HIT be implemented nationally.

The Senators heard from several witnesses. Jack Cochran, Executive Director of the Permanente Federation, urged Congress to consider investment in the nation's healthcare delivery system as a means to stimulate the economy, but cautioned that HIT is not a "silver bullet" to cure all the issues facing US healthcare. He stated the HIT could improve healthcare quality and efficiency and expressed support for federally sanctioned standards. Peter Neuport, Corporate VP of Microsoft Health Solutions, expressed support for providing incentives to invest in HIT. He explained that the incentives should: (1) be technology neutral, (2) reward innovative doctors who use the Internet to communicate with their patients, and (3) focus on making data interoperable. Mary Grealy, President of Health Leadership Council, expressed support for a national health information network. She indicated that such a network requires a funding mechanism to support the IT infrastructure investments necessary to implement HIT and national standards to ensure nationwide interoperability. She opposed prescribing specific technology that ought to be implemented. Valerie Melvin, Director of IT at the Government Accounting Office expressed support for early Congressional oversight of HIT and stated that protecting the privacy of personal electronic health data would be essential to gaining support for the widespread adoption of HIT. Janet Coorgan, CEO and President of the National Quality Forum, stated that federal funding is vital to improving healthcare safety, quality, and affordability.

B. The Senate Judiciary Committee

The Senate Judiciary Committee held a hearing on January 27th to consider the privacy issues implicated by an electronic healthcare system. In particular, the Committee broadly considered the types of privacy and security safeguards necessary to protect consumer privacy in a national electronic health system. Sen. Whitehouse (D-RI) stated that HIT could be a valuable tool in ridding the nation's healthcare system of waste, but that privacy issues implicated by HIT cause him concern. Sen. Leahy (D-VT) highlighted that privacy plays an important role in a person's decision to seek healthcare. He also stated that health records should be computerized within five years. Sens. Hatch (R-UT), Klobuchar (D-MN), and Cardin (D-MD) all expressed support for HIT systems, while recognizing that HIT does raise some privacy issues.

The witnesses expressed support for HIT, but cautioned that the effectiveness of HIT would largely depend on the implementation of privacy and security measures. James Hester, Director of the Health Care Reform Commission of the Vermont Legislature, described Vermont's experience with implementing HIT. He indicated that additional funding might increase HIT implementation, but that consumer confidence in technology influences adoption of HIT. He expressed support for federal guidelines for the states to follow when implementing HIT. Deven McGraw, Director of Health Privacy Project at the Center for Democracy and Technology stated that consumers' privacy concerns impede the implementation of HIT. She called for additional privacy protections and recommended that Congress enact legislation addressing e-health. Adrienne Hahn, Consumer Union, expressed support for developing principles for implementing HIT with safeguards and for the public disclosure of de-identified patient data for research purposes

to improve healthcare. Michael Stokes, Microsoft, explained that trust in HIT could be fostered through transparent practices, consumer control, and data security. He stated that consumers should control how their information may be shared.

John Houston, University of Pittsburgh Medical Center, expressed concern with specific legislation before Congress. He stated that the privacy provisions of the Health Information Technology for Economic and Clinical Health Act would raise costs for providers while creating little benefit for consumers. He suggested imposing limitations on the use of identifiable health information for healthcare operations purposes. He also stated that the burden of de-identifying patient information could deter covered entities from performing certain healthcare functions. David Merritt, Center for Health Transformation and the Gingrich Group, expressed support for providing consumer control and consumer notification of health record breaches, but opposed providing patients with the option to opt out of the de-identification of their information for research purposes.

III. IN THE COURTS

Supreme Court Declines to Review Third Circuit's Ruling that the Child Online Protection Act Is Unconstitutional

On January 21, 2009, the U.S. Supreme Court declined to review the Third Circuit's July 2008 affirmation of a 2007 district court ruling that the Child Online Protection Act ("COPA" or "Act"), 47 U.S.C. § 231, is unconstitutional. The Supreme Court ruling sustains a finding that the Act violates the First and Fifth Amendments because it is impermissibly overbroad and vague. The District Court (or the "Court") held that COPA is an unconstitutional restriction of free speech because it is not the least restrictive alternative for protecting minors from harmful information on the Internet. Instead, the court found that content filtering software is less restrictive than COPA and is at least as effective in protecting minors.

As we first reported in the April 2007 issue of *The Download*:

> COPA is the successor to the Communications Decency Act of 1996, which the U.S. Supreme Court found unconstitutional. With COPA, Congress intended to solve the constitutional defects in the earlier statute. The court, however, issued a permanent injunction against enforcing COPA.
>
> Under COPA, it would be unlawful to knowingly make any communication over the Internet for a commercial purpose that is available to a minor and includes material that is harmful to minors. COPA considers a person to be communicating for commercial purposes only if the person is in the business of making such communications. While this is a broad definition, COPA would have exempted Internet service providers, telecommunications carriers, and providers of "Internet information location tools" from its obligations, and provided an affirmative defense to those who restrict minors' access by requiring use of an individualized access code (*e.g.*, credit card, debit card, or adult access code), an age verification tool, or by any other reasonable measure that is feasible under available technology.

The court held that the statute failed to meet the strict constitutional standards for laws that restrict speech based on content. The court held that COPA is overinclusive, as the terms "commercial purposes" and "engaged in the business" apply to a broad range of Internet speech, covering far more than the commercial pornographers that the government said it intended to cover. The court also found COPA to be overinclusive because it applies to speech that is harmful to all minors—from newborns to age 16—and not just speech that is harmful to older minors. The court also held that COPA is underinclusive. With much of the sexually explicit material on the Internet (perhaps a majority) coming from outside the United States, the court found that COPA's inability to reach this content significantly reduces its effectiveness.

The court held that the affirmative defenses provided by COPA were effectively unavailable because payment cards and digital verification services are not effective in verifying age and, with their deterrent effects on speech, these methods raise their own First Amendment concerns. In addition, the court examined various alternative means of protecting children from harmful material on the Internet and cited significant improvements in content filtering technology, concluding that easy-to-install software is readily available for parents to effectively insulate children from harmful material.

IV. FROM THE STATES

NY Legislator Introduces Online Consumer Protection Act

In the state of New York, Assemblyman Richard L. Brodsky introduced on January 7, 2009, the "Online Consumer Protection Act" (the "bill" or the "Act"), which would permit consumers to elect not to have their data collected online for use to deliver relevant ads to them. As stated in the findings of the bill, the Act would like to make available protections akin to those provided by the National Do Not Call Registry.

The Act would require publishers and advertising networks to acquire a consumer's consent before using a consumer's personally identifiable information ("PII") for purposes of online preference marketing. Under the Act, the term "online preference marketing" would mean "a type of advertisement delivery and reporting whereby data is collected to determine or predict consumer characteristics or preference for use in advertisement delivery on the Internet." Additionally, the Act calls on publishers and advertising networks to provide consumers with the opportunity to opt-out of the use of their non-PII for online marketing purposes. Providing further instruction, the Act also would require publishers and advertising networks to provide notice on their home pages of their advertising delivery activities. The Act would also require advertising networks to make reasonable efforts to protect the data collected for online preference marketing from loss, misuse, alteration, destruction, or improper access.

The Act would empower the Attorney General to enjoin violations of the Act and to impose civil penalties of up to $250 per instance where identifying information is collected in violation of the Act. Additionally, the Act would grant a court authority to triple such damages if the court finds a pattern of violating the Act.

Study Finds that the Privacy Policy of many US Businesses do not Comply with the US Safe Harbor Program

In December 2008, an international report on the U.S. Safe Harbor Agreement ("Safe Harbor") was released. The report was part of a study examining the agreement between European Data Commissioners and the U.S. Department of Commerce, which was signed in 1998. Under the European Union Data Protection Directive ("European Data Directive"), a member state must implement laws that only permit transfers of data from member states to third party countries that provide adequate levels of data protection. The European Union has yet to find that the United States provides an adequate level of data protection. The Safe Harbor therefore allows U.S. businesses to transfer data from Europe to the United States without complying with the European Union member states' requirements governing data transfers. By utilizing the Safe Harbor, a U.S. business can self-certify through the Department of Commerce that it provides an adequate level of privacy protection thereby satisfying the European Data Directive requirement. The report concludes that the Safe Harbor has been ineffective. The study found that only 22% of the registered companies complied with the basic principles of the Safe Harbor; while many organizations claiming to provide adequate data protection actually failed to meet some of the basic requirements. For instance, many companies failed to publicly post a privacy policy or to identify an independent dispute resolution process for consumers.

By making false or misleading statements regarding membership or compliance with the Safe Harbor program, a business may open itself up to an enforcement proceeding by the Federal Trade Commission ("FTC"), which deems false claims as unfair or deceptive acts or practices that are actionable under Section 5 of the FTC Act. Below is a list of common compliance issues related to privacy policies that a business thus ought to consider if it participates in the Safe Harbor:

- Audit your practices to evaluate whether your company complies with the Safe Harbor requirements and that your privacy policy accurately reflects your company's practices.

- Your privacy policy should address all 7 Safe Harbor principles: (1) Notice; (2) Choice; (3) Onward Transfer; (4) Security; (5) Data Integrity; (6) Access; and (7) Enforcement.

- Avoid making false claims regarding the nature of your Safe Harbor certification. For instance, because the Safe Harbor is a self-certification program, refrain from making statements that your company has been certified by the Department of Commerce or the European Union.

- Make your privacy policy readily accessible on the company website.

- Post only the official Safe Harbor Certification Mark provide by the US Department of Commerce on your site rather than using unauthorized logos or marks.

- Immediately preceding the top edge of the mark, provide the following "We self-certify compliance with."

- Include the following links to the US Department of Commerce web site in your privacy policy: (1) http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list and (2) www.export.gov/safeharbor.

- Select with care an independent dispute resolution provider, as required by Safe Harbor Principle 7. Ensure that your membership with such a dispute resolution provider remains current.

- Confirm that your company annually renews its self-certification. The report found that numerous companies claimed compliance, but had not renewed their certification.

---

[1] FTC Staff Report, Self-Regulatory Principles for Online Behavioral Advertising (Feb. 12, 2009).

[2] Id. at 46.

[3] Id. at 25.

[4] Statement of Senator Kennedy in Support of Health Information Technology, available at http://help.senate.gov/Maj_press/2009_01_15.pdf.

Emilio W. Cividanes

Emilio Cividanes concentrates his practice on helping companies meet their privacy obligations in a competitive and global marketplace, and shape the data protection laws and regulations that govern their activities. He has two decades of experience in counseling clients in various industries on how to address privacy challenges to their delivery of services, product development, and other business operations. Mr. Cividanes has lobbied Congress and federal agencies, and participated in the drafting of virtually every federal privacy regulation implemented during the past fourteen years. He has also successfully represented companies in connection with privacy-related litigation and congressional and regulatory investigations. Mr. Cividanes has spoken in the United States, Canada, and Europe on privacy and data protection.

Stuart P. Ingis

Stuart Ingis represents clients in federal privacy and Internet-related legislation and rulemaking proceedings of recent years, including the Controlling the Assault of Non-Solicited Pornography and Marketing Act (Can-SPAM), the Telemarketing Sales Rule (TSR), proceedings pertaining to the financial privacy provisions of the Gramm-Leach-Bliley Act (GLBA), The Electronic Signatures Act (E-Sign), the Children's Online Privacy Protection Act (COPPA), and the Department of Commerce's Safe Harbor Program for compliance with the European Union's Data Protection Directive (the E.U. Directive). Mr. Ingis also represents clients on all aspects of Internet advertising law and policy. In addition, he has been significantly involved on behalf of clients in the Federal Communications Commission's implementation of the landmark Telecommunications Act of 1996 as it applies to the Internet. Mr. Ingis has been involved with Internet law and policy from inception of the commercial Internet. He has spoken in the United States on privacy, electronic commerce and consumer protection, and related issues.

Michael A. Signorelli

Michael Signorelli represents clients in regulatory compliance, transactions and federal privacy, and Internet-related legislation and rulemaking proceedings as a member of the Regulatory group. Mr. Signorelli's experience with federal and consumer protection and privacy issues, regulatory and Federal Trade Commission matters provide his clients a wide breadth of knowledge on which to provide unique solutions.

Tara M. Sugiyama

Tara Sugiyama is an associate in the firm's Regulatory Affairs Practice Group, where she focuses her practice on transactional, regulatory, and policy matters in a broad range of industries. Ms. Sugiyama has significant experience as a mediator and with alternative dispute resolution (ADR) procedures, which informs her approach to assisting clients with ongoing compliance matters. She holds conflict and dispute resolution certificates from the Institute for International Mediation and Conflict Resolution at The Hague, New York University's School of Continuing Education, and the Michigan Supreme Court Administrative Office's General Civil Mediation Training.

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
NINTH FLOOR
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
TWENTY-FIFTH 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 SEVENTH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300