Cyberspace Law Committee

Message from the Chair

As my three-year term as Chair of the Committee comes to a close, it is a good moment to reflect on the Committee and how it continues to have meaning to members of the bar.

When our Cyberspace Law Committee was chartered in the mid-90's, it was a spin-off of the long-standing Uniform Commercial Code Committee. Initially focused on a model agreement for EDI (remember that?), it quickly became the primary place within the Section, and to some extent within the ABA as a whole, for discussion, research and presentation on cutting edge topics involving the Internet, data privacy, and technology related contracting.

As many know, this Committee can no longer claim to be that primary source of "Internet" law and related subjects within the Association. The ABA and our Section are helped by many others inside of the Section, like our SBL Intellectual Property Law Committee, as well as in other Association entities like the Section of Science and Technology, the Section of Intellectual Property, and the Standing Committee on Technology and Information Services. The Association is richer for all of these great groups that contribute to the efforts and our knowledge.

That also means the Cyberspace Law Committee, notwithstanding its more generalized name, has needed to adapt to the changing environment within the ABA. We have in recent years remembered our roots and where we live - We are at heart business lawyers organized to help other business lawyers, and we succeed where we remember who our audience is and what they need. Our committee has crafted, and continues to write, many books and articles that advise business lawyers not just on the technology, but on how they can relate that to a business's legal concerns. We ask our program presenters not to stop just at telling everybody what's really cool in technology, but to take it to the next step and tell companies what it means for them. This is how our Committee can thrive, not by worrying about how others step on our turf, but by sharing the same turf while we present what we see in the way we can do better than anybody else.

And in that task, we have no doubt succeeded. Cyberspace's work product is vibrant, it remains relevant, and our products are consistently viewed as useful (and often entertaining!). We've found new areas in which to relate our skills like payment systems, data security and others even while we build on our traditional points of interest like internet governance and technology contracting. We've developed new ways to present CLE and other substance to members (such as our half-day Institutes presented at the Winter Working Meeting), developed a fuller taxonomy of subjects that comprise Cyberspace Law, and revamped how we provide a survey of that law each year. Our members have been presenting outside of the ABA, including travel to some of the furthest reaches of the world where our members' expertise is invited. And, we've grown in membership within the Section to be one of the Top Ten biggest committees. In short, Cyberspace is changing to the times, succeeding, growing, and fulfilling its mission.

I want to thank all of the dozens of members who have assisted in our ongoing tasks over these last three years, since, as I point out at essentially every event we gather together, it does not happen without you.

Please grant my successor Chair, Jon Rubens of San Francisco, the same courtesy, hard work and dedication you have afforded me while I had this chair. Of course, I should know I don't have to ask that of you - You are doing it already.
Message from the Newsletter Director

Alan S. Wernick
Newsletter Director

The Cyberspace Law Committee ("CLC") explores a wide range of rapidly changing legal disciplines including electronic commerce and contracts, information technology, consumer protection, intellectual property, cyber security & privacy, jurisdiction, Internet governance, mobile media, cloud computing, and online financial activities. This CLC eNewsletter provides our members with an opportunity to help advance members' awareness and understanding of these evolving and dynamic legal issues. Our goal is to make it a useful addition to your practice by helping to make you aware of some of the developments impacting your practice and your clients' businesses, and what these developments mean.

As my three-year term as the Newsletter Director for the ABA Business Law Section Cyberspace Law Committee comes to a close, I want to thank all of the authors and others who have contributed to this publication during my tenure. By contributing to this publication, and to others, these efforts provide a way for us lawyers to give back to the profession and the community we serve by helping further the education and awareness of the rapidly developing and changing areas of law covered by these writings. I ask that you please give my successor whatever assistance you can in providing articles for this publication. Even if you have published an article elsewhere, provided that you own the necessary copyrights to allow for publication by the ABA, we would be interested in hearing from you. Please contact the incoming Editor for the Newsletter if you are interested in submitting an article (in Word format) for publication in this eNewsletter, or if you have any constructive comments or suggestions concerning this newsletter.

Thanks to the other contributors for this issue: Michael Fleming and Marc J. Lederer.

I look forward to hearing from you and reading your articles.

Best regards,

Alan

Alan S. Wernick
Newsletter Director
Partner, FSB FisherBroyles LLP
E-mail: WERNICK@FSBLEGAL.COM

Featured Articles

Vermont AG Settles Data Breach Enforcement Action for $55,000
Marc J. Lederer

On January 21, 2011, the Vermont Attorney General settled an enforcement action against Health Net, Inc. and Health Net of the
Northeast, Inc. (together, "Health Net") for the sum of $55,000. Arising
out of a data breach involving the personal, financial and medical
information of 525 Vermont residents, the enforcement action alleged
violations of Vermont's Security Breach Notice Act, the Health
Insurance Portability and Accountability Act ("HIPAA"), and Vermont's
Consumer Fraud Act.

More...

Use Caution in Technology Contracts
Alan S. Wernick

For nearly three decades my work as an attorney in private practice
and as an arbitrator has involved a wide range of technology contracts.

Before I worked as an attorney I worked as a computer programmer
and as a systems operator. As a programmer, I learned that when I
write a program all it takes is one character to be out of place to cause
a computer program to fail. While that level of exactitude may not be
necessary for drafting or interpreting some contracts, when drafting
computer contracts that divide copyright and other intellectual property
rights, the contract must accurately define the scope of those rights.

More...

HIPAA Goes HITECH with Substantial Civil Money Penalties
Alan S. Wernick

Privacy protection is important in all businesses, including both for-
profit and not-for-profit businesses. In recent developments substantial
civil money penalties have been assessed against privacy violators in
the health care industry. One of the fines was for $4.3 million against
one medical facility, and another was a $1 million fine against a
different hospital.

More...

Who Owns Your Domain Name?
Alan S. Wernick

Domain names are valuable intellectual capital assets in today's
ecommerce economy. However, just because a business has been
using a domain name for years does not mean that the business owns
the domain name.

More...
VERMONT AG SETTLES DATA BREACH ENFORCEMENT ACTION FOR $55,000

BY MARC J. LEDERER

On January 21, 2011, the Vermont Attorney General settled an enforcement action against Health Net, Inc. and Health Net of the Northeast, Inc. (together, “Health Net”) for the sum of $55,000. Arising out of a data breach involving the personal, financial and medical information of 525 Vermont residents, the enforcement action alleged violations of Vermont’s Security Breach Notice Act, the Health Insurance Portability and Accountability Act (“HIPAA”), and Vermont’s Consumer Fraud Act.

Facts of Data Breach

On May 19, 2009, Health Net learned that a portable computer hard drive was missing from the desk of an employee located in its Connecticut office. The missing hard drive contained the personal, financial and medical information of approximately 1.5 million persons, 525 of whom were Vermont residents. Contrary to company policy, the missing hard drive was unencrypted. Health Net began mailing letters giving notice of this breach to affected Vermont residents a little more than six months after the incident occurred, although not all of the letters were received by Vermont residents until more than a year after the hard drive went missing. Health Net claimed that they were unable to identify all of the affected individuals until about six months after the incident occurred.

Vermont’s Enforcement Action

The enforcement action alleged violations of three sets of laws, namely, the Vermont Security Breach Notice Act, HIPAA, and the Vermont Consumer Fraud Act.

This is the first time an enforcement action has been brought under the Vermont Security Breach Notification Act, 9 V.S.A. § 2435, which requires that data collectors notify affected individuals of data breaches involving their personal information “in the most expedient time possible and without unreasonable delay.” The Vermont Attorney General alleged that Health Net did not comply with this requirement because it began mailing out letters more than six months after the incident occurred.

Additionally, the Attorney General alleged that Health Net did not comply with sections of the federally enacted HIPAA, 45 CFR Parts 160 and 164, which require, among other things, that covered entities, such as those who provide health insurance plans, effectively secure an individual’s protected health information.
Vermont’s Consumer Fraud Act, 9 V.S.A. § 2453, prohibits unfair deceptive acts and practices in commerce. The Attorney General alleged that Health Net violated this law by failing to adhere to minimum standards of data security regarding the control, transfer, logging and encryption of protected health information, and by misrepresenting the risk of harm posed to Vermont’s residents in its notification letters.

**Mitigating Factors and Remedial Actions**

The consent decree noted that Health Net represented that it concluded that there was a low risk of harm posed to Vermont residents because:

- the data on the missing hard drive was randomly saved and not searchable;
- information pertaining to Vermont residents represented only a small percentage of the overall data contained in the missing hard drive;
- it took Health Net approximately six months to identify a majority of the members referenced on the missing hard drive; and
- no known identity theft has occurred.

The consent decree also noted that Health Net represented that it has spent in excess of $7 million to remedy this data breach and that it has taken and/or will continue to take the following steps subsequent to the date of the incident:

- providing credit monitoring services, credit restoration services, and up to $1 million in personal internet identity insurance to all affected individuals;
- encrypting all external hard drives and other portable media used to transfer personal information or protected health information;
- encrypting all desktop computers and hard drives of company laptops;
- implementing technology that automatically logs all transfers and actual or attempted access of personal information or protected health information;
- implementing a combination of hardware and software that resides between the email server and the email client that is designed to identify email or attachments containing personal information or protected health information and automatically encrypt email containing such identified information before transmission.

**Settlement Agreement Provisions**

As a result of the agreed-upon settlement with Vermont, Health Net agreed to:
• pay the state of Vermont the amount of $55,000;
• retain a third-party data security auditor to evaluate the extent to which Health Net’s information security programs and practices ensure the security, confidentiality and integrity of personal information and protected health information against future security breaches; and
• provide the Attorney General a written report that describes the auditor’s assessment of Health Net’s information security programs, describes the auditor’s conclusions, identifies any of the auditor’s recommended steps to improve Health Net’s information security programs and practices, and identifies Health Net’s plan for implementing the auditor’s recommended steps. The initial report was to be provided by January 31, 2011, with a follow-up report to be submitted by January 31, 2013.

Conclusion

It should be noted that Health Net’s breach not only resulted in the settlement with the Vermont Attorney General, but it resulted in similar earlier settlements with the Connecticut Attorney General in the amount of $250,000, the Connecticut Insurance Commissioner in the amount of $375,000, and with New York State. These settlements should serve notice to companies that states are actively enforcing their privacy and data breach laws. Accordingly, companies that collect or possess personal information or protected health information would well be advised to take preventive steps such as encryption of such data, and reactive steps to a data breach, such as responsibly expedient notification of affected persons, in order to minimize the damage to their resources and reputation.

About the Author: Marc J. Lederer is a Staff Attorney at Willkie Farr & Gallagher LLP (www.willkie.com). He can be reached via e-mail at mlederer@willkie.com or by phone at 212-728-8624.
USE CAUTION IN TECHNOLOGY CONTRACTS

BY ALAN S. WERNICK

For nearly three decades my work as an attorney in private practice and as an arbitrator has involved a wide range of technology contracts.

Before I worked as an attorney I worked as a computer programmer and as a systems operator. As a programmer, I learned that when I write a program all it takes is one character to be out of place to cause a computer program to fail. While that level of exactitude may not be necessary for drafting or interpreting some contracts, when drafting computer contracts that divide copyright and other intellectual property rights, the contract must accurately define the scope of those rights.

Similarly, when litigating software license agreements it is important to understand the boundaries of the grant of license rights in these agreements before filing a complaint.

As an arbitrator of information technology disputes, I have reviewed contracts drafted by others with my task being to ferret out what the parties intended. This experience has taught me to approach business-critical transactions thoroughly and meticulously. In these business-critical transactions, my client wants to acquire, or deliver, a computer system or a computer program, not a lawsuit.

While there are many cases that speak to the problems that can arise in failed computer system acquisitions or software licensing transaction, a recent case discusses the problems that can arise in the case of a software license grant where the boundaries of the grant of rights are blurry at best.

In HyperQuest, Inc., v. N'Site Solutions, Inc., and Unitrin Direct Insurance Company (USCA, CA7, 2011), N'Site Solutions received a nonexclusive license to copyrighted software called "eDoc" from Quivox Systems. The eDoc software is used to process insurance claims. The N'Site license granted N'Site the right to use the eDoc "... software only within its own facilities; the license conferred no rights to modify the software or to sell it to others."

Quivox subsequently sold its assets to Safelite Group Inc., including the copyrights for the eDoc software.

Safelite then entered into a license agreement with HyperQuest Inc. In the HyperQuest license, the parties acknowledged the existence of the N'Site license and agreed that Safelite retained certain rights to the eDoc software, including the right to use and develop software. In addition, the HyperQuest license stated that "... all right, title and interest in and to the eDoc Software (including, but not limited to, all Intellectual Property Rights) will remain the exclusive property..."
of Safelite and all right, title and interest in and to the HQ Modifications shall vest in Safelite upon creation."

The nexus of the dispute concerned a disagreement between N'Site and HyperQuest over the terms of their licenses. In part, HyperQuest was concerned that N'Site had sold the source code to its modified software to Unitrin Direct Insurance Co. and sued both N'Site and Unitrin for copyright infringement of the copyrighted eDoc software.

The district court found that HyperQuest held only a nonexclusive license and thus lacked statutory standing to sue N'Site and Unitrin for copyright infringement. The court dismissed HyperQuest's lawsuit with prejudice and awarded attorney fees and costs to N'Site and Unitrin as the prevailing party.

In affirming the district court's opinion, the appeals court undertook an extensive analysis of the language in the software license agreements in light of the Copyright Act provision that restricts the set of people who are entitled to bring a civil action for copyright infringement to those who qualify as "[t]he legal or beneficial owner of an exclusive right under a copyright ... ."

The appeals court explained that "HyperQuest's right to recover for N'Site's alleged infringement therefore hinges on its ability to prove that it was an exclusive licensee of at least one of the divisible rights recognized by the [Copyright] act." And the court stated: "[I]t is the substance of the agreement, not the labels that it uses, that controls our analysis."

In holding that HyperQuest was not an exclusive licensee of the copyright, the appeals court stated "... the problem for HyperQuest is that the boundaries between its rights, those that Safelite retained, and those that N'Site was entitled to exercise, are blurry at best."

To underscore the need for critical analysis in the drafting of software licenses, the appeals court added "...just as the use of the word 'exclusive' here and there in the license is not enough to resolve the question of the nature of HyperQuest's interest, the failure to use any particular word is not dispositive. The decision whether Safelite, as the owner of the copyright, has conveyed clear exclusive rights to HyperQuest is one that can be made only after careful analysis of the agreement between the parties."

The bottom line is that in business-critical transactions the parties and their counsel must carefully consider the language and nuances of the agreement, the technology and the law. And remember that someday someone not involved in the transaction (a judge or arbitrator) may be tasked with reading the agreement to determine the parties' intent and legal rights. © COPYRIGHT 2011 ALAN S. WERNICK. WWW.WERNICK.COM.
About The Author: Alan S. Wernick is a lawyer, arbitrator, and writer. He is a partner at FSB FisherBroyles LLP, and is a member of the bars of IL, NY, OH, & DC. Since 1982 Alan’s business law practice has focused in computer law / cyberspace law / information technology law, and intellectual property law, and data privacy/security law transactions. For more than 27 years Alan has served as an arbitrator/mediator in major information technology and intellectual property disputes, as well as an advisor to clients on strategies in handling these types of disputes. He has a background in computer programming and accounting. Additional information about his law firm is available at WWW.FSBLEGAL.COM, and more information about Alan’s practice, lectures, and publications is available at WWW.WERNICK.COM. His email address is WERNICK@FSBLEGAL.COM and his phone number is 847.786.1005.
HIPAA GOES HITECH WITH SUBSTANTIAL CIVIL MONEY PENALTIES

BY ALAN S. WERNICK

Privacy protection is important in all businesses, including both for-profit and not-for-profit businesses. In recent developments substantial civil money penalties have been assessed against privacy violators in the health care industry. One of the fines was for $4.3 million against one medical facility, and another was a $1 million fine against a different hospital.

Perhaps you have heard anecdotal stories about the neighborhood intersection where neighbors start to notice that increased traffic through the intersection presents increased risks to children and others in the area. The neighbors complain to the local governing authority, but nothing happens until a few significant personal injuries occur in the intersection, and only then traffic signals are installed or law enforcement begins more closely monitoring the intersection. Whether or not those anecdotal stories are true, in some organizations, large and small, the approach to privacy is often like that hypothetical intersection—an accident waiting to happen.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act and amended the penalty amounts established under HIPAA, combine to form a strong statutory foundation for organizations handling health care information to pause and give serious consideration (and resources) to prevent privacy violations.

A review of the Department of Health & Human Services (HHS) Oct. 20, 2010, and Feb. 4, 2011, letters to Cignet Health Center (Cignet) in Maryland present an unfortunately all too common response that some businesses take towards privacy—the classic ostrich (i.e., head in the sand, avoidance) strategy. Consider the following partial excerpts from the Oct. 20, 2010, Notice of Proposed Determination letter from the Office for Civil Rights in HHS to Cignet:

“4. Cignet did not respond to the 41 individuals ... who requested copies of their medical records maintained by Cignet.

7. Cignet did not respond to OCR’s written notification of the investigations, numerous follow-up attempts to contact Cignet by telephone, or to two subsequent letters ... informing Cignet of its obligation at 45 C.F.R. §164.524 to provide the individuals access to obtain a copy of the protected health
information about them in the designated record sets (medical records) maintained by Cignet.

10. On June 26, 2009, OCR issued a subpoena duces tecum directing Cignet to produce the medical records of the individuals in the first group of 11 complaints by no later than July 27, 2009. The subpoena was delivered to Cignet by United States Postal Service certified mail, return receipt requested, and was received by Cignet’s agent on June 29, 2009.

11. Cignet failed to produce the medical records as directed in the subpoena and failed to respond to OCR in any way regarding the June 26, 2009 subpoena.

14. On February 4, 2010, through the representation of the Department of Justice, Civil Division, Federal Programs Branch, OCR filed a petition to enforce its subpoena duces tecum in the United States District Court for the District of Maryland .... The Court issued an order for Cignet to show cause and scheduled a hearing for March 29, 2010. Cignet did not appear at the hearing, did not respond to the petition and did not defend the action.”

The OCR Notice of Proposed Determination further informed Cignet of the proposed civil money penalties (“CMP”) of $4,351,600 and Cignet’s right to a hearing. As the Feb. 4, 2011, OCR Notice of Final Determination to Cignet states, Cignet failed to request the hearing or file an appeal. Thus, the civil money penalty was final.

The Feb. 22, 2011, HHS news release states, “‘Covered entities and business associates must uphold their responsibility to provide patients with access to their medical records, and adhere closely to all of HIPAA’s requirements,’ said OCR Director Georgina Verdugo. ‘The U.S. Department of Health and Human Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules.’”

As privacy violations continue to increase both in the health care and other industries, enforcement efforts will increase. As these violations approach a tipping point, more federal and state agencies will enforce the law against violators, and more civil money penalties will be imposed.

The bottom line is that all businesses today need to be proactive stewards of data subject to privacy laws, and seek knowledgeable counsel in dealing with information technology law and data privacy law issues.

© COPYRIGHT 2011 ALAN S. WERNICK. WWW.WERNICK.COM.
About The Author: Alan S. Wernick is a lawyer, arbitrator, and writer. He is a partner at FSB FisherBroyles LLP, and is a member of the bars of IL, NY, OH, & DC. Since 1982 Alan’s business law practice has focused in computer law / cyberspace law / information technology law, and intellectual property law, and data privacy/security law transactions. For more than 27 years Alan has served as an arbitrator/mediator in major information technology and intellectual property disputes, as well as an advisor to clients on strategies in handling these types of disputes. He has a background in computer programming and accounting. Additional information about his law firm is available at WWW.FSBLEGAL.COM, and more information about Alan’s practice, lectures, and publications is available at WWW.WERNICK.COM. His email address is WERNICK@FSBLEGAL.COM and his phone number is 847.786.1005.
WHO OWNS YOUR DOMAIN NAME?

BY ALAN S. WERNICK

Domain names are valuable intellectual capital assets in today's ecommerce economy. However, just because a business has been using a domain name for years does not mean that the business owns the domain name.

Case study

A recent case, DSPT International, Inc., vs. Lucky Nahum (USCA, 9th Cir., Oct. 27, 2010), provides an example where a business went to court to establish ownership rights and damages when its website was replaced by a page directing visitors to another website.

DSPT designs, manufactures and imports men's clothing. In 1999, DSPT created an EQ brand. Around that time its owner, Dorigo, decided to create a website. Dorigo had brought into the business a friend, Nahum, whose brother was a part-time website designer. DSPT's website, eq-Italy.com, was developed by Nahum's brother in consultation with Dorigo. However, Nahum registered the website in his own name.

In the fall of 2005, Nahum decided to leave DSPT and join a competitor. About a month later, "...DSPT's website mysteriously disappeared. If a customer typed eq-Italy.com into his web browser, instead of seeing DSPT's clothing line, all he saw was a screen saying, 'All fashion-related questions to be referred to Lucky Nahum at: lnahum@yahoo.com.'" Nahum "had inserted that sentence in order to get ... [DSPT] ...to pay him funds that were due to him."

As soon as DSPT became aware of what happened, DSPT requested Nahum to give back the website, but he refused.

Per the court: "Sales plummeted and inventory was left over in the spring from the very bad fall. 2004 had been good and the first quarter of 2005 was the best ever, but the last quarter of 2005, and all of 2006, were disastrous. A lot of inventory had to be sold below cost. DSPT spent $31,572.72, plus a great deal of time, writing to customers to explain the situation and replacing its website and the stationery that referred customers to eq-Italy.com."

In affirming the trial court's decision, the 9th Circuit looked to the Anti-Cybersquatting Consumer Protection Act, which creates a civil liability basis for "cyberpiracy" when a plaintiff proves that (1) the defendant registered, trafficked in or used a domain name; (2) the domain name is identical or confusingly similar to a protected mark owned by the plaintiff; and (3) the defendant acted "with bad faith intent to profit from that mark."
No dispute existed over the first element — Nahum registered the domain name and was refusing to transfer it to DSPT.

Regarding the second element, the court held that DSPT had common-law trademark rights and a jury could reasonably conclude that the domain name eq-Italy.com is "confusingly similar" to the EQ mark.

For the third element, the court reviewed "bad faith intent" and noted that while there was no evidence of any wrongdoing by Nahum's original domain name registration, his subsequent behavior — using the domain name as leverage against DSPT for his claim of commissions it owed — elevated the behavior to "use" of the domain name "with bad faith intent to profit" therefrom. "As for whether use to get leverage in a business dispute can establish a violation, the statutory factors for 'bad faith intent' establish that it can."

Concluding that the jury verdict awarding DSPT $152,000 in damages was supported by the evidence, the appeals court stated: "Even if a domain name was put up innocently and used properly for years, a person is liable under 15 U.S.C. § 1125(d) if he subsequently uses the domain name with a bad faith intent to profit from the protected mark by holding the domain name for ransom."

**One preventive step**

When was the last time you did a Whois query to check the status of your or your client's Internet domain name? The information for the administrative contact and the technical contact are used to manage and maintain the domain name.

Let's say an employee registers a domain name for the business using the employee's business address. When an employee leaves the company his e-mail address is shut down and e-mails sent to that address become undeliverable. What happens when an issue arises concerning that domain name and e-mails sent never get through? The domain name might be lost or other costs incurred.

If your business owns a website domain name, consider using generic e-mail addresses for the domain name registrant, technical and other contact information. Then, set up this generic address to automatically forward any incoming e-mails to several individuals in the company who can respond appropriately to any activity concerning the domain name.

The bottom line is that just because a business uses a website, it cannot assume that it in fact owns the website. If you have not had one done recently, consider having a website legal audit done by an attorney knowledgeable in information technology and intellectual property law. The cost of this preventive legal audit will be far less (both in money and management time)
than the costs if you have to go to court, as did DSPT, to establish your legal rights to your domain name.

© COPYRIGHT 2011 ALAN S. WERNICK. WWW.WERNICK.COM.

About The Author: Alan S. Wernick is a lawyer, arbitrator, and writer. He is a partner at FSB FisherBroyles LLP, and is a member of the bars of IL, NY, OH, & DC. Since 1982 Alan’s business law practice has focused in computer law / cyberspace law / information technology law, and intellectual property law, and data privacy/security law transactions. For more than 27 years Alan has served as an arbitrator/mediator in major information technology and intellectual property disputes, as well as an advisor to clients on strategies in handling these types of disputes. He has a background in computer programming and accounting. Additional information about his law firm is available at WWW.FSBLEGAL.COM, and more information about Alan’s practice, lectures, and publications is available at WWW.WERNICK.COM. His email address is WERNICK@FSBLEGAL.COM and his phone number is 847.786.1005.

###