Members:

January is always an exciting time for the Cyberspace Law Committee, as it more or less kicks off our year of work. Of course, the big event for many of us is our annual Winter Working Meeting, with its panoply of substantive breakouts and social events. This year, as we visit Austin, Texas, we will also try out the first year of what we hope will be an ongoing tradition - The Cyberspace Law Institute, a roughly four hour continuing legal education seminar focused on topics we love to talk about such as internet governance, cyber-security, privacy and intellectual property. This year's program is brought to us with assistance from the Austin law firm of McGinnis, Loehrige & Kilgore, L.L.P., our legal colleagues in iTechLaw, and our friends at Dell Computer.

The 2010 Survey of Cyberspace Law was published by The Business Lawyer in November, and as usual it presents the most current developments in our area of practice. Members should already have their paper copies from the Section, and members can also download a copy from the ABA website. We begin anew in January to solicit articles for the 2011 survey, and I truly commend this as an opportunity for members, particularly young lawyers, to be published in a well-respected legal journal.

Our Section publishes a monthly electronic magazine, Business Law Today. As a member of the editorial board of the magazine, I am always looking for authors who wish to draft magazine-like articles (3000 or so words and NO FOOTNOTES!) on current topics. The magazine's turn-around time is fairly quick, and this is another great opportunity to be published and placed on the screens of over 55,000 business lawyers.

The Cyberspace Law Committee is a prolific producer of CLE programming for the Section's Spring and Annual meeting efforts. We will be primary sponsor of three programs at the Spring Meeting in Boston this April. The programming director, Jon Rubens, will be seeking proposals soon for presentation at the Annual Meeting in August in Toronto. The Business Law Section continues to enhance and build on its webinar and non-traditional CLE presentation systems, and is actively seeking good programming for those media as well. If you are interested in presenting to an audience of lawyers who need to understand the complexities of the law of cyberspace, there are many opportunities for you here.

And, we will also publish this newsletter, and seek your input. Like the magazine, it seeks informal writing on current topics of interest in cyberspace law. We will also consider articles you may have previously published in your firm's newsletter or the like - the point is to get content to our members! Contact Alan Wernick with your ideas or your articles.

In short, the Committee offers you many active systems to get your own words distributed to the world. This annual cycle of activities, repeating year after year for well over a decade, is a record of the hard work of our members who find the legal issues of the internet, software and 'cyberspace' to fascinate and keep us busy. I hope to see your name on one of our work products in the coming year.

Michael Fleming
Chair, Cyberspace Law Committee

http://apps.americanbar.org/buslaw/committees/CL320000pub/newsletter/201101/
Message from the Newsletter Director

Alan S. Wernick
Newsletter Director

The Cyberspace Law Committee explores a wide range of rapidly changing legal disciplines including electronic commerce and contracts, consumer protection, intellectual property, cyber security & privacy, jurisdiction, internet governance, and online financial activities. This CCL 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. Please contact me if you are interested in submitting articles 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, Marc J. Lederer, Marie-Andrée Weiss.

I look forward to hearing from you.

Alan S. Wernick
Newsletter Director

Featured Articles

The UK’S ICO Issues First Fines for Privacy Violations
Marc J. Lederer

On November 24, 2010, the UK Information Commissioner for the first time used its powers to issue monetary penalties and fined two organizations as a result of data breaches they committed. A4E Limited was fined a total of £60,000 following the theft of an unencrypted laptop containing the personal data of thousands of persons, and the Hertfordshire County Council was fined £100,000 for accidentally faxing highly sensitive information to the wrong recipients. This article will focus on the circumstances of the A4E Limited fine.


More...
A View from the U.S. Supreme Court on Technology Usage Policies
Alan S. Wernick

In today’s environment, employees (and independent contractors) frequently do their jobs using technology provided by the hiring party. Examples of that technology include computers, software, Internet, e-mails, cell phones and pagers. The businesses that provide technology to their employees or independent contractors often will set forth policies regarding the use of the technology. It is time again to review those policies in light of a recent U.S. Supreme Court decision.

More...

Social Media Sites and Underwriting
Marie-Andrée Weiss

If you are in the market for life insurance, and would like to get a good rate, maybe you should stop checking web pages featuring fatty foods, fast cars, or share your concerns about your high blood pressure on social media sites. On the other hand, if you usually surf the web to find recipes whose main ingredients are tofu and flax seeds, or if you registered online for the 10K meet of your local Masters Swimming Team, you may be pleasantly surprised by the lower premium offer extended to you by insurance companies.

More...

Warning Cloud
Alan S. Wernick

There are many benefits available to companies that convert their information technology systems to cloud computing. However, there are many legal issues to consider before converting. Issues that are frequently overlooked include the e-discovery implications and attorney-client privilege.

More...
THE UK’S ICO ISSUES FIRST FINES FOR PRIVACY VIOLATIONS

By Marc J. Lederer

On November 24, 2010, the UK Information Commissioner for the first time used its powers to issue monetary penalties and fined two organizations as a result of data breaches they committed. A4E Limited was fined a total of £60,000 following the theft of an unencrypted laptop containing the personal data of thousands of persons, and the Hertfordshire County Council was fined £100,000 for accidentally faxing highly sensitive information to the wrong recipients. This article will focus on the circumstances of the A4E Limited fine.

Background

The UK Information Commissioner (“ICO”) is empowered under the UK Data Protection Act (the "UK Act") to ensure that organizations comply with the requirements of the UK Act. The UK Act consists of eight principles aimed at ensuring that personal information is:

• Fairly and lawfully processed
• Processed for limited purposes
• Adequate, relevant and not excessive
• Accurate and up to date
• Not kept for longer than necessary
• Processed in line with a data subject’s rights
• Secure
• Not transferred to other countries without adequate protection

The ICO is given various enforcement powers under the UK Act, including the authorization to issue monetary penalties of up to £500,000 for serious breaches of the UK Act. When imposing penalties, the ICO considers the particular circumstances of the nature and the severity of the data breach.
Facts

In the case of A4E Limited, one of its employees was issued a company laptop for the purpose of working on a report remotely from the organization’s office. While working at home with the laptop, the employee loaded personal data and sensitive personal data of 24,000 clients onto the laptop from the central secure servers. The laptop was password protected but was not encrypted. Thereafter, the laptop was stolen from the employee’s home. It appeared that the thief may have attempted to access the data but was unsuccessful. The laptop was never recovered.

Discussion

The ICO found that A4E Limited contravened the seventh data principle of ensuring that personal information is secure from accidental loss or destruction by failing to take appropriate technical and organizational measures against the accidental loss of personal data held on the laptop computer, such as by encrypting the laptop computer and providing the employee with security devices for the laptop computer, for example, a Kensington lock or a cable. The ICO found that the contravention was serious because the security measures taken did not ensure an adequate level of security appropriate to the harm that might result from the accidental loss and the nature of the data to be protected. In addition, the ICO found that the data subjects suffered substantial distress evidenced by the number of complaints and other contacts that A4E Limited received from data subjects. Moreover, the ICO concluded that A4E Limited knew or should have known that the personal information was at risk, and that failing to secure the personal information would cause substantial damage or substantial distress. In fact, the ICO had published very relevant guidance for this type of situation in 2007 in which it stated that: “There have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect data, enforcement action will be pursued”. Therefore, taking into account the circumstances of the nature and severity of the data breach, including the financial resources of A4E Limited to pay a monetary penalty without causing undue financial hardship, the ICO issued a fine of £60,000 (to be reduced to £48,000 for early payment).

Conclusion

Data breaches are not uncommon occurrences for companies these days. With the amount of data maintained and transmitted by organizations, it is extremely difficult to guard against every circumstance that may lead to a data breach, whether it be as a result of an
accident or due to criminal wrongdoing. With these fines, the ICO has put companies on notice that it will issue penalties for serious data breaches, especially when they can be prevented by taking reasonable security precautions. It should be noted that the ICO is not alone with respect to punishing companies for data breaches, as regulators both in other European Union nations and in the United States are enforcing their data breach laws and holding organizations accountable. Accordingly, it is incumbent upon organizations to be proactive in minimizing opportunities for data breaches by developing comprehensive privacy policies and procedures as well by providing proper training of personnel and by having the necessary IT infrastructure in place.

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.

___


iii The data included information such as debt/welfare/employment, the name, zip code, date of birth and gender of the data subject together with whether or not the data subject was a single parent, caregiver, a victim of violence, ex-offender, youth offender or gypsy traveler.
A VIEW FROM THE U.S. SUPREME COURT ON TECHNOLOGY USAGE POLICIES

By Alan S. Wernick

In today's environment, employees (and independent contractors) frequently do their jobs using technology provided by the hiring party. Examples of that technology include computers, software, Internet, e-mails, cell phones and pagers. The businesses that provide technology to their employees or independent contractors often will set forth policies regarding the use of the technology. It is time again to review those policies in light of a recent U.S. Supreme Court decision.

In Quon v. Arch Wireless Operating Co., Inc., et al. (June 17, 2010), the U.S. Supreme Court examines technology usage policies and Fourth Amendment implications.

The Fourth Amendment of the U.S. Constitution states, “The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated.” This is not limited to criminal investigations. As the court notes, "The amendment guarantees the privacy, dignity and security of persons against certain arbitrary and invasive acts by officers of the government, without regard to whether the government actor is investigating [a] crime or performing another function.”

The Quon case involves several police officers (respondents) who were issued pagers by their employer (petitioner), the Ontario, Calif., Police Department, and who used the pagers for personal text message communications. The department requested pager bills as part of its auditing of the invoices, and Arch Wireless Operating Co., Inc. (Arch), which contracted to provide text-messaging services, furnished them to the Police Department, along with copies of the text messages sent by the respondents. Some of the messages were "personal in nature and often sexually explicit.”

The Supreme Court, in reversing the 9th U.S. Circuit Court of Appeals, held that the Police Department did not violate the employees’ Fourth Amendment rights when it searched the respondents’ text messages. The court noted that even if Quon had a reasonable expectation of privacy in his messages, the department did not necessarily violate the Fourth Amendment by obtaining and reviewing the transcript of the text messages.

As a general matter, warrantless searches, the court reminds us, are per se unreasonable under the Fourth Amendment: “There are ‘a few specifically established and well-delineated exceptions’ to that general rule, and one of the exceptions looks to the ‘special needs’ of the work place.” The court states that "when conducted for a 'non investigatory, work-related purpos[e]' or for the ‘investigatio[n] of work-related misconduct,' a government employer's warrantless search is reasonable if it is ‘justified at its inception’ and if ‘the
measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search.”

Essentially, the court took a practical approach that the Police Department's auditing of the text messages to see if the billing (work versus personal charges) was accurate (that is, both the department and the officers were paying the appropriate amount for the text messaging service), was for a legitimate "noninvestigatory work-related purpose," and therefore a reasonable search under the Fourth Amendment.

In considering whether the search was too intrusive, the court states it has “repeatedly refused to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.” That rationale “could raise insuperable barriers to the exercise of virtually all search-and-seizure powers’ …because "judges engaged in post-hoc evaluations of government conduct can almost always imagine some alternative means by which the objectives of the government might have been accomplished."

The court goes on to say, “The analytic errors of the court of appeals in this case illustrate the necessity of this principle. Even assuming there were ways that OPD could have performed the search that would have been less intrusive, it does not follow that the search as conducted was unreasonable.”

Companies should take a fresh look at their policies regarding corporate computer, software, Internet, text messaging and e-mail systems that contain the company's business data, including evaluating any employer's right of inspection in light of the fl v. 14 decision.

As Judge Richard A. Posner in Muick v. Glenayre Electronics, (U.S.C.A., 7th Circuit, 2002) observed, “The laptops were Glenayre’s [the employer’s] property, and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible.”

In the event of a dispute, the facts surrounding that inspection will have to pass the scrutiny of the Fourth Amendment. Now is a good time to review your organization's technology policies. Ignoring these preventive legal procedures can create additional, and unexpected, legal risks or expenses to the business.

© COPYRIGHT 2010 ALAN S. WERNICK. WWW.WERNICK.COM.
About The Author: Alan S. Wernick 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. For more than 26 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.
SOCIAL MEDIA SITES AND UNDERWRITING

By Marie-Andrée Weiss

If you are in the market for life insurance, and would like to get a good rate, maybe you should stop checking web pages featuring fatty foods, fast cars, or share your concerns about your high blood pressure on social media sites. On the other hand, if you usually surf the web to find recipes whose main ingredients are tofu and flax seeds, or if you registered online for the 10K meet of your local Masters Swimming Team, you may be pleasantly surprised by the lower premium offer extended to you by insurance companies.

The Wall Street Journal reported in November 20101 that insurance companies are using the digital files of personal information gathered by data aggregation companies to evaluate whether an insurance prospect is a high risk or not. A life insurer is interested in knowing whether the prospect has a higher than average or below average life expectancy. In order to assess the risks, insurers traditionally relied on physical exams and questionnaires during the life insurance underwriting process. However, this traditional method is costly. Licensed health professionals employed by the insurer may have to visit the prospect’s house to gather medical samples, perform drug testing, and gather the answers to a medical questionnaire.

A more cost-effective method is “predictive modeling.” Is the prospect likely to develop a serious medical condition? Does he engage in dangerous activities? Predictive modeling mines data compiled by data collection companies to find the answer. This method is not only used by insurers, but also by banks or credit card companies to assess whether it would be profitable to extend an offer to a particular prospect.

Insurers and banks may also use network analysis programs and sites which analyze social network data. Specialized software and data aggregating sites are available to companies eager to use the constantly-updated flow of social media data to forecast marketing trends, identify their customers’ needs, and predict risks. Jeremiah Owyang, a marketing professional, wrote a blog post last June where he predicted that insurance companies will soon use social media sites data to assess which rate should be extended to a prospect.2 According to an article recently published by The Economist, some financial firms identify who could be a borrowing risk by using SAS software3, which analyzes both an applicant’s social network and her Internal Revenue Service records. The article also mentions that some insurers are offering better premiums to banks using such software to protect themselves.4 However, insurers tempted to use social media sites to check whether a claim is legitimate may be well advised not to move to have access to the social media account of the interested party, as courts may view this as a “fishing expedition,” the terms used in November 2010 by the New York...
Appellate Division Court, which affirmed a lower court order denying as overly broad an insurer’s motion to access the Facebook Page of a woman who had been injured in an accident involving one of the company’s insured. However, the lower court had “abused its discretion in prohibiting defendant from seeking disclosure of plaintiff's Facebook account at a future date.”5

Even if this method lowers both cost of underwriting borne by companies and perhaps the cost of premiums borne by consumers, it does also raise privacy concerns. Is this practice regulated by any U.S. law? The Wall Street Journal’s article quoted Rebecca Kuehn of the Federal Trade Commission as saying that using information sold by marketing-database firms during the life insurance application process would “raise questions” as to whether such practice would be subject to the Fair Credit Reporting Act (FCRA). Indeed, the FCRA defines a consumer report as “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness (...) credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (...) credit or insurance to be used primarily for personal, family, or household purposes.” 15 U.S.C. § 1681a(d) (1)(A). Data collection firms fit the definition of a “consumer reporting agency” under the FCRA as being “any person which, for monetary fees (...) regularly engages (...) in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties (...).”15 U.S.C. § 1681a(f).

If this data is subject to the FCRA, then a banker or an insurer who would take an adverse action based on this data would have to disclose it to the prospect. Such an adverse action under the FCRA is the “denial or cancellation of, an increase in any charge for, or a reduction or other adverse or unfavorable change in the terms of coverage or amount of, any insurance, existing or applied for, in connection with the underwriting of insurance.” 15 U.S.C. § 1681k(1)(B)(i).

One of the privacy round tables held by the Federal Trade Commission (FTC) this year explored the privacy implications of social networking, and noted that, as the number of third-party applications enabled to access social media information grows, it is important that consumers understand how their data is being shared.6 Following the roundtables, the FTC recently published a preliminary staff report proposing a normative framework applying to companies collecting data and sharing consumer data.7 One of the report’s propositions is to provide consumers with simple ways to express their data privacy choices. Companies should also make their data practices more transparent to consumers.

It will be interesting to see if, as social media users become more aware that information they so readily share on social media sites may be eventually be used by business
companies, they will use the full range of privacy settings already offered by social media sites, and even ask for tighter privacy options, or whether federal and/or state laws will be enacted to regulate the use by banks or insurers of social media data for underwriting purposes.

About the Author: Marie-Andrée Weiss is a New York attorney and solo practitioner focusing on IP and Privacy. She can be reached via e-mail at marie-andree@maw-law.com or by phone at 917-509-2376.

1 http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html
2 http://www.web-strategist.com/blog/2010/06/14/how-insurance-companies-will-influence-rates-based-on-your-tweets
4 http://www.economist.com/node/16910031
6 http://www.ftc.gov/bcp/workshops/privacypolicies/PrivacyRoundtable_Jan2010_Transcript.pdf, p. 22
There are many benefits available to companies that convert their information technology systems to cloud computing. However, there are many legal issues to consider before converting. Issues that are frequently overlooked include the e-discovery implications and attorney-client privilege.

INTRODUCTION

Cloud computing is one of the current waves in information technology. Cloud computing allows the user to transfer many (if not all) of the user’s computing functions performed via personal computer applications (and the user’s data) to a remote location maintained by the cloud computing service provider. The functions are then accessible by the user through high-speed connections.

Secure Internet connectivity can allow the user access to the cloud virtually anywhere the user has Internet access—whether it’s the user’s headquarters, an off-site clinic, store, factory, a remote warehouse, a doctor’s office, a hotel, a convention center, or home.

LEGAL ISSUES ABOUND

Some companies are hesitant to venture into cloud computing because of the security issues and regulatory compliance issues. Examples of legal issues include the following:

1. E-discovery: What is the impact on evidentiary issues in litigation when the user’s data is in the cloud? What data from others is available to your expert?

2. Attorney-client privilege: What impact will storing client confidential materials in the cloud have on the attorney-client privilege? Will the attorney-client privilege be waived by placing such materials in a cloud computing environment?

3. Privacy, both of the user’s data and the user’s customer’s data: Who establishes, maintains, and audits the access to the user’s data and applications in the cloud?

4. Jurisdiction: In case of a data breach, which law applies—that law where the customer is located, that law where the cloud services vendor is located, or that law governing the network or server farm where the data resides? Who has the legal obligation to prepare and send a notice of a data breach?
5. Licensing: If the user uses proprietary third-party applications, do the software license agreements allow for cloud computing usage? This would include not only the scope of use coverage, but other issues as well (e.g., representations and warranties, software maintenance, and upgrade issues).

6. Limitations of liability: If the user signs up for the cloud-computing services through a click-wrap agreement, the terms and conditions are not negotiated. While the click-wrap agreement may be okay in some instances, the cloud-services users may have legal and/or business difficulties with some of the terms and conditions (e.g., the user may find the limitations of the vendor’s liability an unacceptable business risk and desire to negotiate different levels and/or triggers of vendor liability).

7. Service level agreements: What are the appropriate service-level agreement terms and conditions? What metric will be used to measure performance in the cloud?

8. Termination: What happens to the user’s data if the cloud-services vendor goes out of business or is acquired by a competitor to the user? If the vendor simply goes out of business, the user could be without access to its business-critical data as well as the applications needed to process that data. Depending on the user’s industry, such a scenario could trigger numerous regulatory concerns.

9. Audits: How will the user audit the user’s data stored in a cloud-computing environment? How will data quality and data integrity be audited and maintained while in the cloud?

This is not an exhaustive list of all the legal issues, the analysis and determination of which will depend on many factors. These factors include the applicable technology, as well as the business and legal environment for the user and the cloud services vendor.

**PRIVACY**

Privacy in cloud computing is a threshold issue that must be properly addressed in a cloud-computing environment. It cannot be considered in the same light as when all of the computer hardware and software are located at a facility owned and/or operated by the user, and the hardware and software maintained by the user.

For instance, if the user is in an industry, such as the health industry, that relies on substantial data storage:

1. Will the cloud-computing vendor execute a business associate’s agreement appropriate to the cloud-computing model?
2. What are the risk allocations in the event of a data breach?

3. Who has the obligation to respond in the event of a data breach (e.g., the user or the cloud computing platform provider)? Which laws apply?

4. How are access controls established and maintained?

CLOUDY DISCOVERY

What happens to your data when it’s stored in a cloud computing environment?

While there are many nuances to contracting for cloud computing, one aspect frequently overlooked is the e-discovery implications. Often e-discovery is not considered during the contract negotiations because it typically does not arise until some time after the contract has been executed by the parties. For example, when a third party asks the user to produce data stored in the cloud, the request may come as an e-discovery request in the context of a dispute between the user and a third party, or from third parties claiming to have an interest in data that the user controls or has the right to control in the cloud computing environment.

E-mail messages are a familiar example of data that may be stored in a cloud computing environment and may be one of the deliverables in a cloud computing contract. There are many examples of e-mail storage presently being done in a cloud computing environment. In the course of any litigation, access to e-mails will be a necessary part of the e-discovery process. Structuring the cloud computing contract to address the e-discovery issues will save the user time and money when the user has to access those e-mails for compliance or e-discovery purposes.

SUMMARY AND CONCLUSION

The cloud two years from now will be very different in terms of accessibility and risks than it is today. And today, not all cloud systems are alike. For instance, some systems include hardware oriented firewalls, redundant backups, and sophisticated security systems, while some do not. However, because of the potential for IT cost savings and increased accessibility, many companies will not want to wait before jumping into the cloud.

The bottom line is parties should (1) plan ahead in structuring their cloud computing contracts using knowledgeable legal counsel and (2) consider the many legal issues including, without limitation, the e-discovery implications in the design of the deliverables.
Cloud computing offers many efficiencies and potential cost-savings for the business community. It must be approached cautiously, however, lest the cloud become a fog in which the user loses his way and falls from the cloud into a legal quagmire.

© COPYRIGHT 2010 ALAN S. WERNICK. WWW.WERNICK.COM.

About The Author: Alan S. Wernick 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. For more than 26 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.