State Bar of Michigan

Michigan IT Lawyer

A Publication of the State Bar of Michigan Information Technology Law Section

http://www.michbar.org/it

Table of Contents

May 2012 ▪ Vol. 29, Issue 3

Michigan IT Lawyer is published every other month. Previously published issues of the *Michigan IT Lawyer*, and its predecessor the *Michigan Computer Lawyer*, are available at http://www.michbar.org/it/newsletters.cfm. If you have an article you would like considered for publication, send a copy to:

Michael Gallo
2700 Renshaw Drive
Troy, Michigan 48085
e-mail: michael@gallo.us.com

Bits and Bytes from the Chair

By Charlie Bieneman, *Rader, Fishman & Grauer PLLC*

It was great to see everyone who turned out for our Spring Networking Event, held in conjunction with the Detroitnet.org IT networking organization on May 17. For those of you who could not make it, I hope you will put this event on the calendar next year. It was a great opportunity to mingle with folks in the industry we serve—and I enjoyed speaking with some of my fellow lawyers as well!

Section activities tend to wane during the summer months, but we are busy planning this year's fall seminar, to be held on September 27, 2012, and the St. John's Inn in Plymouth. Before too long, you'll receive more information from our partners at ICLE about this event. However, our lineup speakers and programs is set, and we are looking forward to another great seminar.

Best wishes to everyone for a great summer!

Charlie Bieneman

2011-2012 IT Law Section Chair

2012
Edward F. Langs Writing Award

Essay Competition Rules

1. Awards will be given to up to three student essays, which in the opinion of the judges make the most significant contribution to the knowledge and understanding of information technology law. Factors to be taken into consideration include: originality; timeliness of the subject; depth of research; accuracy; readability; and the potential for impact on the law.
2. Essay must be original, deemed to be of publishing quality, and must not have been submitted to any other contest within the previous 12 months.
3. Essay must be typed, double spaced, at least ten pages in length, must contain proper citations listed as either endnotes or footnotes, and must have left, right, top, and bottom margins of one inch.
4. Essay must include the submitter's name, email address, mailing address, telephone number, and school attended.
5. A total of $1,500 in US dollars shall be divided between the award winning essays, and all rights to award winning essays shall become the property of the State Bar of Michigan.
6. The Information Technology Section of the State Bar of Michigan reserves the right to make editorial changes, and to publish award winning essays in the Section's newsletter, the *Michigan IT Lawyer.*
7. Essay must be submitted as a Microsoft Word document, postmarked by June 30, 2012, and emailed to *dsyrowik@brookskushman.com*. ■

Save the Date for Our Fall Seminar!

September 27, 2012 ■ St. John's Inn in Plymouth
Details to come.

The *Michigan IT Lawyer* is pleased to present "Cloud Cover: Navigating the Foggy Legal Framework Surrounding Cloud Computing" by Megan Nicholls, a winner of the 2011 Edward F. Langs Writing Award competition, and a graduate of the University of Windsor School of Law.

The statements made and opinions expressed in this essay are strictly those of the author, and not the State Bar of Michigan or the Information Technology Law Section. Comments regarding this article can be forwarded to the *Michigan IT Lawyer*, care of *michael@gallo.us.com*. Enjoy!

Cloud Cover: Navigating the Foggy Legal Framework Surrounding Cloud Computing

By Megan Nicholls

> "[For cloud computing] there is no code of conduct. There's no standard. There's nothing that safeguards privacy and establishes rules of the road."
>
> - *Senator John Kerry, chair of the Subcommittee on Communications, Technology and the Internet*[1]

Take cover! Cloud computing has taken the Internet by storm. Internet services offered by cloud computing service providers are increasingly being used by both individual and corporate users, who are attracted to the efficiency and low cost of the services. However, the cloud model of Internet data storage, management and display is also the source of many privacy concerns. This paper will argue that although the legislation surrounding cloud computing services is ambiguous and complex, users must not wait for legislative reform, but instead must take action to protect their data by carefully selecting the cloud services they use and by keeping sensitive information inaccessible to the general public online. Firstly, the paper will argue that the legal framework surrounding cloud computing is complex and outdated. Secondly, it will explain that although the legal framework for cloud computing is antiquated, legislative reform is not likely to happen any time soon. Thirdly, it will argue that users can best protect themselves by carefully selecting terms of service agreements and considering various options before uploading information into the cloud. Finally, it will conclude that although cloud computing seems to raise brand new privacy concerns, these issues and the practical solutions to protecting user information on the cloud are not terribly new.

I. The Legal Framework for Cloud Computing is Ambiguous

Cloud computing is the ability to run applications and store data on a service provider's computers over the Internet, rather than on a person's laptop or desktop computer.[2] This model of Internet use allows users to access and jointly edit or review documents online, and shifts the costs of purchasing processing power and storage capacity onto cloud providers.[3] The cloud provider can install upgrades required by technology vendors and complete maintenance for all of its users simultaneously.[4] Because of these significant advantages, cloud computing is creating intense competition within the technology industry, and individual users as well as corporate users are catching on to its potential for efficiency and cost reductions. Many universities, law firms, and big businesses are switching to data management and storage on cloud computing websites, and individual consumers are continuing to build their online databases on webmail, personal health records, calendar, contact management, word processing and social media sites. Yet the legal framework for this new technology has not developed quickly enough to offer users concrete protections for information stored in this "cloud."

The *Stored Communications Act* is the primary federal source of online privacy protections, and regulates disclosure of information by cloud service providers. It is a component of the broader *Electronic Communications Privacy Act* ("ECPA"), and was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.[5] While the Fourth Amendment only applies to government actors, the SCA narrows the opportunities for private actors to disclose information.[6] In general, the SCA prevents providers of Internet communications services from divulging private communications to certain entities and individuals, by regulating the relationship between government investigators and service providers in possession of user's private information.[7] The SCA's provisions have four main implications for cloud computing. Firstly, the statute limits the government's right to compel providers to disclose information in their possession about their customers and subscribers.[8] Secondly, the statute limits the right of an Internet service provider ("ISP") to disclose information about customers and subscribers to the government voluntarily.[9] Thirdly, the SCA prevents third party litigants from obtaining information stored on a cloud server by service of a subpoena duces tecum.[10]

The SCA is a difficult statute to understand and apply, because it was enacted in 1986 and relies on a model of electronic mail and Internet activity that is generations behind current practice and technology.[11] Despite the rapid evolution of computer and network technology since the SCA's adoption, its language has remained surprisingly static.[12] As a result, adapting the SCA's language has fallen largely on the courts.[13] The legislation is not built around clear principles that are intended to easily accommodate future changes in technology; instead, Congress chose to draft a complex statute based on the operation of early computer networks; courts must therefore extract operating principles from the tangled legal framework to apply it to modern computing.[14] Courts have struggled to find a place within this framework for communications made on cloud servers, leaving users and providers sometimes in the dark with respect to their rights and obligations.

When drafting the SCA, Congress based its provisions on two types of services popular at the time, and categorized them as "electronic communications services", or ECS, and "remote communications services", or RCS.[15] However, Internet technology has come a long way since this model of communication, and the SCA no longer suits modern models of Internet use such as cloud computing services. The ECS category of provisions were based primarily on early electronic mail systems, which involved a fragmented delivery system in which communications were slowly transmitted between the computer servers operated by email providers.[16] Each provider's servers would temporarily store an email until transmitting it along to its next waypoint.[17] After an email reached its destination, the recipient would use a dial-up modem to connect to her email provider and download the message to her computer.[18] Alternatively, some providers would conveniently put the messages onto paper and then deposit them into the regular postal system.[19] Although email is no longer communicated in this way, the provisions of the SCA have not been amended to reflect the updated technology.

The SCA defines an ECS provider as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[20] A service provider must satisfy two requirements to qualify as ECS: firstly, it must provide users the ability to send or receive "electronic communications", which is defined broadly to include nearly any form or style of communication, including signs, signals, writings, images, sounds, data or intelligence of any nature.[21] Secondly, the service provider must hold the electronic communication in "electronic storage", which is defined very narrowly to mean temporary, intermediate storage incidental to the electronic transmission of the communication and copies made by the service provider for backup protection.[22] These provisions reflect the original email delivery system at the time of the SCA's creation, which required multiple providers to store communications briefly before forwarding them on to their next destination or while awaiting download by the recipient.[23] Cloud computing, by contrast, allows users to access their emails without downloading them.

The second category of provisions deal with remote communications services or RCS, and were designed to address third-party service providers that offered sophisticated and convenient computing services to subscribers and customers from remote facilities.[24] Since buying a lot of processing or storage capacity was so expensive, organizations began to outsource these functions to a service provider.[25] These companies would transmit their data for processing either to a third-party service provider's personnel or directly transfer it to the provider's remote computer.[26] This service was marketed to businesses of all sizes, including hospitals, banks and many others, as opposed to individual consumers, and Congress wanted to protect these entities against the prying eyes of RCS providers.[27] This type of service is similar in substance to the cloud services offered to corporations today, but different in form. Cloud servers allow corporate users to store data online, rather than on the cloud provider's hard drive.

Remote communications services provide computer storage or processing services to the public by means of an electronic communications system.[28] An electronic communications system is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[29] To qualify as RCS, the provider cannot be authorized to access the customer's content for purposes of providing any services other than storage or computer processing.[30] These requirements perfectly describe the nature of the commercial relationship that existed at the time of the SCA's adoption between the outsourced computing providers and their business clientele.[31] However, these provisions have not been modified to suit the new form of data storage on the cloud.

The distinction between RCS and ECS affects the level of privacy protection extended to the service provider or the communication involved. If a service is categorized as ECS, the SCA provides two levels of privacy protection depending on whether disclosure of the communication is voluntary or compelled by the government.[32] The first tier deals with voluntary disclosure by the service provider. Providers of ECS to the public ordinarily cannot disclose content-based information unless they meet one of eight exceptions; for example, if the communication's sender or recipient consents to the disclosure, or when the disclosure is necessary for the "protection of the rights or property of the provider," then the provider can disclose the information.[33] The second tier of ECS protections deal with government-compelled disclosures.[34] A probable cause search warrant is required if the communication has been in "electronic storage" on the provider's service for 180 days or less.[35] After 180 days, the government may use an alternative legal process with a lower causal threshold (which is similar to the requirements of RCS disclosure described below).[36]

If the communication is defined as an RCS, then the same two-tiered approach is applied, but with fewer privacy protections than for communications held by an ECS.[37] An RCS provider may voluntarily disclose a customer's content-based data in compliance with one of the same eight statutory exceptions as an ECS.[38] Data stored in RCS for any duration may be accessed by the government through an order requiring only "reasonable grounds to believe" the data is "relevant and material to an ongoing criminal investigation."[39] Information stored on an RCS provider is very easily obtained by a simple subpoena for government entities, whereas to obtain information stored on an ECS provider for less than 180 days, a probable cause warrant is required which is less easily obtained.

Although the provisions of the SCA perfectly suited the technology at the time, it does not suit cloud computing servers or services. For example, many cloud computing services would seem to fail to qualify for the heightened privacy protections provided to ECS.[40] Firstly, this is because ECS must give users the ability to send or receive electronic communications and not all cloud services provide this service (e.g. photo sharing or word processing applications do not typically have webmail capabilities).[41] Secondly, ECS communications must be held in "electronic storage", which is limited to either storage of a temporary and intermediate nature that is incidental to the electronic transmission or storage of the communication by the ECS provider to provide backup protection.[42] Cloud services typically do not do either: storage is offered to provide long-term data retention and are usually meant to be the final repository for customer's data, rather than backup protection.[43]

The RCS provisions in the SCA initially seem like a better fit for cloud providers, because Congress originally added these provisions to address outsourced computer processing and data storage.[44] In many ways, cloud computing is a reversion to this practice.[45] Recall that to qualify as RCS, a cloud provider must firstly publicly offer 'computer storage or processing services' over a network, and most cloud providers do offer storage or processing services.[46] In addition, cloud providers typically meet three of the SCA's additional requirements for RCS communications: the data must contain content; the data must be carried or maintained on behalf of a subscriber or customer; and the data must be electronically transmitted to the provider.[47] However, cloud services would seem to fail to meet the SCA's two remaining requirements: the customer's data must be transmitted to the cloud provider solely for the purpose of providing storage or computer processing services, and the cloud provider must be authorized to access the contents of any such communications for the sole purposes of providing storage or computer processing.[48] Thus, cloud computing services do not truly qualify for either ECS or RCS protection under the SCA.

However, courts seem to have relaxed the strict requirements of both ECS and RCS to fit cloud computing into this antiquated framework. Webmail services allow customers to send or receive email, and therefore satisfy the first prong of ECS communications.[49] Every court to consider the issue agrees that as to unopened emails, the second ECS prong is satisfied because unopened mail is stored temporarily until the user opens it.[50] However, electronic communication is complete when opened or downloaded by its intended recipient, so the provider is no longer temporarily storing the opened email.[51] Some circuits have held that a webmail

provider becomes ECS with respect to opened mail because the user is said to be holding it as backup protection, meeting one of the definitions of electronic storage.[52] However, there is a split among federal courts as this creative reasoning, and such an interpretation has received substantial judicial and academic criticism.[53] Although this reasoning has recently been confirmed in *Crispin v. Christian Audigier*, whether or not courts will continue characterize webmail as ECS is as yet unsettled.[54]

Whether other types of cloud services will be afforded the protections of the SCA is also unclear. Courts have determined that the same provider can act in both an ECS and RCS capacity, and the services it provides must be considered individually to determine which standard is applicable in a given situation.[55] For example, social media websites like Facebook and MySpace provide private messaging services as well as forums for bulletin-board style messaging. The Court in *Crispin* grappled to determine whether bulletin-board comments and wall posts on Facebook and MySpace were ECS or RCS communications under the SCA.[56] In this case, Morrow J. recognized that the legislative history of the SCA suggests that Congress wanted to protect electronic communications that are configured to be private, such as private electronic bulletin boards, and therefore extended the definition of ECS to postings on electronic bulletin boards.[57] The Court reasoned that a user's passive decision not to delete a communication after it has been read by the user renders that communication stored for backup purposes, just as an undeleted email is said to be held for backup purposes.[58] However, as we have seen, this reasoning is controversial and will not necessarily be followed.

Crispin also held that in the alternative, the Facebook and Myspace wall postings could also be RCS communications, relying on the 2008 case *Viacom v. YouTube*.[59] In *YouTube*, the Court held that the video storing and displaying website YouTube qualifies as an RCS when storing private videos and other user content on its website, despite that the communications were not maintained "solely" for the purpose of storage.[60] The *YouTube* Court looked at the fact that YouTube's terms of service agreement allowed it to access and delete potentially infringing private videos, and held that this access was permissible under the SCA because it occurred in connection with YouTube's provision of alleged storage services.[61] This reasoning was probably a reference to the exception allowing RCS providers to access a customer's data when it is necessarily incident to the rendition of the service.[62] In *Crispin*, the Court similarly noted that the bulletin board messages were not maintained by the websites solely for the purpose of storage, but admitted that the *YouTube* case could not be distinguished.[63] The Court's admission highlights the difficulty judges have in applying the SCA to cloud services.

In support of the argument that bulletin board postings could be RCS communications, Morrow J. pointed out that a storage service necessarily requires a retrieval mechanism to be useful, and thus that such display function is necessarily incident to the rendition of service.[64] Although a large number of users, i.e. all of a user's Facebook friends, might access the storage and attendant retrieval/ display mechanism, the number of users who can access documents in storage has no legal significance.[65] The Court noted that basing a rule on the number of users who can access information would result in arbitrary line-drawing, and would likely have the anomalous result of corporations such as law firms, which may have thousands of employees who can access documents in storage, being excluded from the statute.[66] Finally, the Court recalled that the SCA does not limit storage to retention for the benefit of the user only.[67] Whether or not these arguments will be extended to bulletin-board messages stored on a corporate cloud service remains to be seen.

However, even ECS or RCS protection under the SCA may not ultimately protect a user's information from disclosure sought by a third party. In *Crispin*, the Court determined that the absence of a provision concerning a civil subpoena in the SCA can be interpreted as reflecting Congress' desire to protect users' data from the reach of private litigants, and that such an interpretation is consistent with the principles of statutory construction and the supporting case law.[68] However, under 18 U.S.C. § 2511(2)(g), any person can intercept or access the communication if the information at issue is "readily accessible to the general public."[69] The Court further held that private messaging and webmail services are inherently private such that stored messages are not readily accessible to the general public, and therefore are protected by the SCA.[70] However, it remanded the decision to determine whether the general public had access to the Facebook wall and MySpaces postings.[71] The Court noted that the magistrate judge would be able to determine whether the information at issue was readily accessible to the public by examining the plaintiff's privacy settings.[72] Although the outcome of this case is not yet available, the *Crispin* decision illustrates the weight that courts are likely to place on privacy agreements and user privacy settings rather than rely on the complexities of the SCA.

Courts may even read the privacy agreements as extending "public access" to the private messaging services on such websites. For example, in *Romano v. Steelcase*, the

Supreme Court of New York examined whether the plaintiff's current and historical Facebook and MySpace pages and accounts (including all deleted pages and related information) were discoverable by a private litigant.[73] Although the Court noted that the SCA prohibits an entity from disclosing such information without the consent of the owner of the account, it did not discuss whether the Facebook or MySpace accounts were RCS or ECS under the SCA, nor did it examine whether the information was readily accessible to the public under § 2511(2)(g).[74] Instead, the Court granted the defendant access to the plaintiff's social media website pages, because the public portions of the sites contained material and necessary evidence, and therefore the private portions of her sites probably contained further material and necessary evidence.[75] The case illustrates that not all courts consider public and private information similarly, and that some courts misunderstand or misapply the SCA's provisions and the intent of Congress in extending privacy protections to information stored in the cloud.

Fourth Amendment arguments are not likely to protect any information stored on a cloud server. For example, the plaintiff in *Romano* failed in her argument that her Fourth Amendment right to privacy would be breached if the pages were disclosed.[76] In determining whether a right to privacy exists via the Fourth Amendment, courts examine whether a person has exhibited an actual (subjective) expectation of privacy and whether the expectation is one that society is prepared to recognize as reasonable.[77] However, the Fourth Amendment does not typically protect the privacy of information disclosed to a third party.[78] In arriving at its conclusion that the plaintiff had no reasonable expectation of privacy over her Facebook and MySpace pages, the *Romano* Court noted that neither Facebook nor MySpace guarantee complete privacy, and that the terms of service agreements of both services explicitly warn the user that such forums are public spaces and that the information might become publicly available.[79] When the plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding any privacy settings she may have chosen.[80] *Romano* emphasizes that courts can be unwilling to extend Fourth Amendment privacy rights to cloud users because this information has been disclosed to a third party.

It should be noted that non-content based information is generally entitled to little protection under the SCA as well as the Fourth Amendment. In the seminal case on non-content information under the Fourth Amendment, the U.S. Supreme Court held in *Smith v. Maryland* that there existed no expectation of privacy for dialed numbers.[81] Non-content information for Internet transactions, such as logs maintained by a network server, is slightly better protected by the SCA.[82] For both ECS and RCS communications, providers cannot disclose a user's non-content information unless the provider meets one of six exceptions.[83] Yet only a simple subpoena is required to compel basic subscriber information, such as name or IP address, or transaction information, such as time and date of the email's transmission.[84]

It should also be noted that the USA PATRIOT Act, enacted in 2001 and amended in 2005, includes provisions allowing the FBI to access any business record.[85] A court order is required, but the FBI's authority is sufficient to extend to a record maintained by a cloud provider.[86] There is some dispute as to whether the PATRIOT Act weakens some of the privacy protections previously found in the SCA, and generally expand the government's ability to compel disclosure, or whether the PATRIOT Act simply codified existing judicial precedent and therefore did not truly affect users of their civil liberties.[87]

In sum, the legislation and case law do not offer much certainty for emerging cloud services. For example, courts are likely to be faced in the near future with the question of whether advertising-based cloud services will qualify for protection under the SCA. Contextual advertising allows a marketing campaign to target a specific audience based on the content a website visitor is accessing.[88] On one hand, cloud services powered by contextual advertising require access to content other than for storage or computer processing as the SCA requires for RCS protection, making such services technically ineligible for this category.[89] On the other hand, the *Crispin* decision indicates that courts may be willing to interpret such access for other purposes as "necessarily incident" to the rendition of the service provided. Advertising-based cloud models such as Google arguably wouldn't exist if not for the advertisers which make the sites free and easily accessible by many users. However, whether courts will strictly interpret the provisions of the SCA or stretch its rigid framework to fit cloud servers is still up in the air.

II. Reform of the SCA

The relative uncertainty of the privacy protections extended by the SCA and the courts' application of the statute concerns many critics and scholars, who advocate heavily for reform. Morrow J. admitted great difficulty in interpreting the SCA, noting that the complexity of the provisions in the statute is compounded by the fact that the SCA was written prior to the advent of the Internet and the World Wide Web.[90] It concluded that the existing statutory framework

is ill-suited to address modern forms of communication like Facebook and MySpace.[91] The Court ultimately warned that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as these will remain a confusing and uncertain area of the law.[92] Indeed, courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.

The confusing dichotomy between ECS and RCS communications is not the only reason the SCA is criticized. Firstly, critics argue that Congress should raise the threshold the government must satisfy to compel the contents of certain Internet communications, particularly with respect to RCS communications, which are discoverable with a mere subpoena.[93] Secondly, currently the delay period for notice to users that the information is sought is ninety days; critics argue that this delay period should be shortened so that notice delayed does not become notice denied.[94] Thirdly, the SCA currently has no suppression remedy where information is unlawfully sought, which many feel is unjust.[95] Fourthly, many feel that the SCA should be modified to require police officer presence during searches of email at ECS or RCS centers, just as is required at U.S. postal offices.[96] Finally, the SCA has been incorrectly applied in several cases.[97] For example, courts have incorrectly extended the SCA to regulate the placement of cookies on home computers by holding that a home computer is a provider of ECS that falls within the SCA.[98] The Courts in *Crispin*, *Romano* and many others struggle with the logic and conflated case law that attends the SCA. Critics continue to offer suggestions about how to improve this legislation, yet Congress has failed to act. Why?

There are several legislative, judicial, and social obstacles to the SCA's reform. Firstly, the SCA does an arguably adequate job of protecting user information where it is worthy of protection. Although its provisions are complex, courts like the one in *Crispin* have interpreted the SCA in light of the legislative intent of Congress in drafting the statute, and have creatively stretched its provisions to suit modern technology. The uncertainties in the statute for emerging technologies are not so great as to halt its progress, a concern that Congress recognized in drafting the SCA.[99] Cloud services continue to prosper and grow in popularity, and certainly social media networks show no signs of extinction any time soon. This may suggest that users are at least relatively satisfied with the legal protections of their personal and corporate information. However, it may also suggest that users have taken their data protection into their own hands, rather than rely on the SCA and relevant case law for protection.

Secondly, many cloud users are comfortable with revealing personal information over the Internet, in exchange for free services and targeted advertising.[100] Most recognize that information sharing is what makes social networks useful and are willing to contribute in exchange for exposure to others' personal information. Many users (including teenagers and young adults) are aware that such information is not protected by law and are restricting access to their online profiles in response.[101] Thirdly, recent congressional actions are reducing the sphere of individual privacy in the wake of 9/11 terrorist attacks, rather than seeking its expansion.[102] This suggests that Congress is in no rush to modify the statute to expand its privacy protections for Internet users. Fourthly, Congress has a limited capacity to pursue new legislation, and politicians struggle to focus Congress' finite attention on a particular issue; therefore seeking incremental or even moderate change is very hard to achieve.[103] The demographics of Congress make it unlikely that their members are well-positioned to determine society's expectations, especially about emerging technologies.[104] Advocates for change must ensure that elected officials and judges understand the technology and its implications for individual privacy before they can secure their assistance in changing the status quo.[105] For these reasons, despite the complexities of the SCA and the relevant framework for determining privacy protections for cloud users, the SCA is not likely to be amended any time soon.[106]

III. Cloud Users Must Protect Themselves in Other Ways

Rather than wait for legislative reform, cloud users of the future should make savvy decisions on the marketplace by choosing cloud providers with terms of service agreements that favor the protection of the user's information, and by not posting sensitive information on cloud services. There are generally three categories of terms of service agreements.[107] The first is where the cloud provider has explicit authority to access a customer's data for marketing or other purposes (for example, Google).[108] The second category gives the provider vague authority to potentially access a customer's data for purposes beyond the primary services (for example, YouTube, whose agreement allows access to remove infringing videos).[109] The third category explicitly prohibits the provider from accessing a customer's data for any purpose other than providing a specific service (e.g. Remember the Milk, an online task management system).[110]

The first category is the least likely to be afforded the protections of the SCA, since users have notice that the

information stored on the server may be accessed by third parties. The second category may protect information stored on the servers, depending on how the information is used. Courts will likely have to determine whether the location of the information exposed the communication to third parties. The third category is most likely to be protected by the SCA, since the user has a reasonable expectation that the information will not be exposed to a third party. However, if the information is deemed to be posted in a "public" location, even the terms of service agreement is not likely to protect the information. In short, courts will have to delve into each cloud provider's operations and practices as well as consider the type and location of the communication to determine whether the information should be protected.[111] Users should therefore choose wisely when storing or sending information using a cloud provider. Unless the privacy agreement explicitly prohibits the cloud provider from accessing the user information for any reason, information stored on the Internet is likely subject to disclosure by a private litigant. Users should be also cognizant of where they are posting the information, and whether the general public is likely to have access to the post.

Several other considerations must be made when deciding whether to use a cloud service. Users should be aware that terms of service agreements can often be changed by cloud providers at any time, sometimes without notice, which could affect the level of protection afforded to the communications on the cloud. Information sent to a cloud service can also be stored in foreign jurisdictions, exposing the communication to very different discovery and privacy standards. Users should read the agreement to determine whether storage of data may occur in a different jurisdiction, and if concerned, should insist on data retention only in the U.S. Many cloud providers also limit or disclaim any liability for data that is lost or stolen from the cloud servers. Users should therefore not use the cloud service as the sole source of backup for sensitive or important information, and corporate users should definitely have a backup system when storing client data. Cloud providers also often reserve the right to modify any content retained in the cloud, and the ability to modify or alter content can impact a user's ability to remove data from a cloud or switch to another cloud service provider. In addition, cloud providers too are susceptible to bankruptcy, and the hard drives could be purchased by an unknown third party (or sold on eBay!). Finally, some jurisdictions require computer technicians to report criminal activity they find when repairing or otherwise servicing computers, so users should be aware of this requirement when posting personal or client data.

If negotiating an airtight privacy agreement isn't available, users have many other options. For those concerned about what user information the cloud already holds, Senator John Kerry, chair of the Subcommittee on Communications, Technology and the Internet, is introducing a new bill on Internet privacy which would require companies to make sure all the information a cloud provider knows about a user is secured from hackers and to let the user inspect the data, correct mistakes and opt out of being tracked.[112] This would allow users to remove existing information they are concerned about. Although this bill may not be passed with brevity, it signals that piecemeal legislation may be passed to supplement the SCA with respect to privacy protections for cloud users. Although such fragmented legislation is not ideal, it may be the best option given that the SCA is not likely to be reformed soon. As to future cloud communications, the Federal Trade Commission has released a report that calls upon the major browsers to come up with a do-not-track mechanism that allows people to choose not to have their information collected by companies they are not directly doing business with.[113]

As can tend to happen with technology, however, the marketplace has addressed these concerns before the law has. Google Dashboard is a response to threats to consumer privacy which allows users to review the personal data Google has stored for them, delete it, and alter future collection policies.[114] Dashboard leaves Google in the prime position of being able to say honestly that it doesn't control user data, while still delivering beneficial services based on that data.[115] However, critics argue that it will never be used by the vast majority of Google users, because if accessing useful services or completing work more efficiently requires some privacy concessions, the public gladly concedes.[116] Ultimately, the user information stored in the cloud is not altogether very interesting, unless an adversary has reason to use it against a user.

The clouds thicken, however, when corporate entities join the cloud by moving data into cloud servers. Since corporations like law firms and banks are dealing with other people's information, the stakes are higher. A survey from the Deloitte Forensic center (a think tank that explores ways to mitigate the effects of illegal and unethical business practices) found that only 9 percent of the business surveyed believed they were well-prepared to electronically capture and store digital information generated on cloud computing programs or on software-as-a-service applications.[117] But the significantly lower cost of using the cloud is driving the data's migration beyond the firewall: the data has left the building.[118] Corporations

simply cannot afford to wait for legislative reform to protect their data on the cloud, and must make savvy decisions when selecting a cloud service and uploading data onto the cloud.

To limit their liability for wrongful disclosure, corporate entities can include an indemnification provision for losses that are the fault of the provider, and may consider getting "cyber-insurance" in the event of information loss or disclosure.[119] Corporations should create data maps to track how information travels through the firm's network and determine how that information would interact with the systems of a cloud provider.[120] Although these precautions may seem daunting, in many ways there is more risk associated with corporations attempting to secure and protect its own computing infrastructure as compared to leveraging the expertise of a cloud provider. The risks to a corporation's data – including potential data loss, security breaches or government disclosure demands – exist whether the corporation uses cloud computing or on-premise computing.

IV. Conclusion

We have seen that the legal framework surrounding cloud computing is ambiguous and complex. We have also seen that while the SCA is in need of reform, it is not likely to happen any time soon. Thirdly, we have seen that despite these legal ambiguities, users have plenty of options on the marketplace to protect their information on the cloud. While cloud computing may seem revolutionary, the privacy considerations this emerging technology raises for both corporations as well as individuals are not terribly new. The SCA was created to extend Fourth Amendment protections to information stored and communicated on the Internet, and those basic principles inherent in Fourth Amendment analyses remain largely the same. Non-content information is not protected, nor is information disclosed to a third party. The case law suggests that courts are likely to extend these basic principles to communications disclosed on emerging technologies. Users must simply ensure that the information they disclose on the cloud server is not sensitive, unless they are confident that the terms of service agreements are airtight. Therefore while the legal framework is ambiguous at this stage, users have the opportunity to protect themselves by making savvy decisions on the marketplace.

The idea behind cloud computing is also not terribly new. Recall that the practice reverts back to the old days of computer processing when data was processed and stored in a mainframe and users accessed this central mainframe through "dumb" terminals. Further, cloud services based on contextual advertising can be seen as modern versions of the phone book, junk mail and telemarketing, wherein organizations take and profit from personal information. Worrying about disclosure of personal information is also old news: in 1890, Louis Brandeis argued that printing a photograph without the subject's permission inflicts mental pain and distress far greater than could be inflicted by mere bodily harm.[121] Yet just as we have become accustomed to being photographed without our express permission, and have accepted that our images and information in the hands of commercial organizations is not necessarily abhorrent, cloud users will likely get used to having their laundry – dirty or not – aired amongst the clouds, and take steps to protect it only when truly necessary. ■

Legislation

18 U.S.C. §§ 2510(15), 2511(2)(g), 2702-3

50 U.S.C. § 1862

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860-68

Jurisprudence

Buckley H. Crispin v. Christian Audigier Inc., 717 F.Supp.2d 965 (2010) (Dist. Ct.)

Flagg v. City of Detroit, 252 F.R.D. 346, 366 (E.D. Mich. 2008)

In re Subpoena Duces Tecum to AOL, LLC, 550 F.Supp.2d 606 (E.D. Va. 2008)

Romano v. Steelcase Inc., 30 Misc. 3d 426, 907 N.Y.S.2d 650

Smith v. Maryland, 442 U.S. 735 (1979)

Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003), *amended by* 359 F.3d 1066, 1075-76 (9th Cir. 2004)

Viacom Int'l Inc. v. YouTube, Inc., 253 F.R.D. 256 (S.D.N.Y. 2008)

Secondary Sources

Matt Asay, *Google Privacy Controls: Most People Won't Care*, The Open Road (November 5, 2009) (available at http://news.cnet.com/8301-13505_3-10390456-16.html)

Joe Dysart, As Bulging Client Data Heads for the Cloud, Law Firms Ready for a Storm, ABA Journal (April 1, 2011) (available at http://www.abajournal.com/news/article/as_bulging_client_data_heads_for_the_cloud_law_firms_ready_for_a_storm/)

Kimberly S. Cuccia, *Have You Seen my Inbox? Government Oversteps the Fourth Amendment Again: Goodbye Telephones, Hello Email*, Valparaiso University Law Review, 2009

Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, World Privacy Forum 1 (2009)

Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's guide to Amending It*, 72 G.W.L.R. 1208 (2004)

Privacy 2.0: Give a little, Take a Little, The Economist (January 28 2010) (available at http://www.economist.com/node/15350984)

William Jeremy Robison, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195 (2010)

Joel Stein, *Your Data, Yourself*, Time Magazine 40 (March 21, 2011)

Endnotes

1 Joel Stein, *Your Data, Yourself*, Time Magazine 40, 41 (March 21, 2011).

2 William Jeremy Robison, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1199 (2010).

3 *Id*. at 1202.

4 *Id*.

5 Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 G.W.L.R. 1208, 1209-1213 (2004).

6 Robinson, *supra* n. 2 at 1228.

7 Kerr, *supra* n. 5 at 1212, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860-68.

8 18 U.S.C. § 2703.

9 *Id*. at § 2702.

10 *Buckley H. Crispin v. Christian Audigier Inc*., 717 F.Supp.2d 965 (2010) (Dist. Ct.) ("*Crispin*"); see also *Viacom Int'l Inc. v. YouTube, Inc*., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) ("*YouTube*"); *In re Subpoena Duces Tecum to AOL*, LLC, 550 F.Supp.2d 606, 611-12 (E.D. Va. 2008); *Flagg v. City of Detroit*, 252 F.R.D. 346, 366 (E.D. Mich. 2008).

11 Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, World Privacy Forum 1, 12 (2009).

12 Robison, *supra* n. 2, at 1196.

13 *Id.*

14 *Id.* at 1205.

15 *Id.* at 1205.

16 *Id.*

17 *Id.*

18 *Id.* at 1206.

19 *Id.*

20 18 U.S.C. § 2510(15).

21 Robison, *supra* n. 2 at 1206.

22 *Id.*

23 *Id.*

24 *Id.*

25 *Id.* at 1207.

26 *Id.*

27 *Id.*

28 18 U.S.C § 2711(2).

29 *Id.* at § 2510(14).

30 Robison, *supra* n. 2 at 1207.

31 *Id.*

32 *Id.*

33 *Id.* at 1208.

34 *Id.*

35 Kerr, *supra* n. 5 at 6.

36 *Id.*

37 Robison, *supra* n. 2 at 1208.

38 18 U.S.C. 2702(b).

39 *Id.* at § 2703(d).

40 *Id.*

41 *Id.*

42 *Id.*

43 *Id.* at 1210.

44 *Id.* at 1212.

45 *Id.*

46 *Id.*

47 *Id.*

48 *Id.*

49 Robison, *supra* n. 2 at 1210.

50 *Id.*

51 *Id.*

52 *Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003), *amended by* 359 F.3d 1066, 1075-76 (9th Cir. 2004).

53 Robison, *supra* n. 2 at 1211.

54 *Crispin*, *supra* nt. 10.

55 *Id.* at 1210-1211.

56 *Id.*

57 *Id.* at 981.

58 *Id.* at 989.

59 *Id.*

60 *YouTube, supra* n. 10.

61 *Id.*

62 Robison, *supra* n. 2 at 1219.

63 *Crispin*, *supra* n. 10 at 990.

64 *Id.*

65 *Id.*

66 *Id.*

67 *Id.*

68 *Id.*

69 18 U.S.C. § 2511(2)(g).

70 *Crispin*, *supra* n. 10 at 991.

71 *Id.*

72 *Id.*

73 *Romano v. Steelcase Inc*., 907 N.Y.S.2d 650, 30 Misc. 3d 426.

74 *Id.* at 652.

75 *Romano, supra* n. 73.

76 *Id.*

77 *Id.* at 432.

78 Robison, *supra* n. 2 at 1226.

79 *Romano*, *supra* n. 73 at 656.

80 *Id.*

81 442 U.S. 735 (1979).

82 Kerr, *supra* n. 5 at 1219.

83 18 U.S.C. § 2703(d).

84 *Id.* at § 2703(b).

85 50 U.S.C. § 1862.

86 Gellman, *supra* n. 11 at 14.

87 *Id.*

88 Robison, *supra* n. 2 at 1213.

89 *Id.* at 1214.

90 *Crispin*, *supra* n. 10 at 989.

91 *Id.*

92 *Id.*

93 Kerr, *supra* n. 6 at 16.

94 *Id*. at 19.

95 *Id*. at 16.

96 Kimberly S. Cuccia, *Have You Seen my Inbox? Government Oversteps the Fourth Amendment Again: Goodbye Telephones, Hello Email*, Valparaiso University Law Review, 2009 at 10.

97 Kerr, *supra* n. 5 at 4.

98 *Id*.

99 Robison, *supra* n. 2 at 1225.

100 *Id.* at 1238.

101 *Privacy 2.0: Give a little, Take a Little*, The Economist (January 28 2010) (available at http://www.economist.com/node/15350984) at 2.

102 Robison, *supra* n. 2 at 1234.

103 *Id.* at 1235.

104 *Id.* at 1236.

105 *Id.*

106 *Id.* at 1234; Kerr, *supra* n. 5 at 18.

107 Robison, *supra* n. 2 at 1215.

108 *Id.*

109 *Id.*

110 *Id.* at 1217.

111 *Id.* at 1221.

112 Stein, *supra* n. 1 at 41.

113 Stein, *supra* n. 1 at 42.

114 Matt Asay, *Google Privacy Controls: Most People Won't Care*, The Open Road (November 5, 2009) (available at http://news.cnet.com/8301-13505_3-10390456-16.html) at 2.

115 *Id*. at 3.

116 *Id*. at 2.

117 Joe Dysart, As Bulging Client Data Heads for the Cloud, Law Firms Ready for a Storm, ABA Journal (April 1, 2011) (available at http://www.abajournal.com/news/article/as_bulging_client_data_heads_for_the_cloud_law_firms_ready_for_a_storm/).

118 *Id*. at 2.

119 *Id*. at 4.

120 *Id*.

121 Stein, *supra* nt. 1 at 42.

Mission Statement Information Technology Law Section, State Bar of Michigan

The purposes of the Section are to review, comment upon, and appraise members of the State Bar of Michigan and others of developments in the law relating to information technology, including:

(a) the protection of intellectual and other proprietary rights;

(b) sale, leasing, distribution, provision, and use of, hardware, software, services, and technology, including computer and data processing equipment, computer software and services, games and gaming, information processing, programming, and computer networks;

(c) electronic commerce

(d) electronic implementation of governmental and other non-commercial functions;

(e) the Internet and other networks; and

(f) associated contract and tort liabilities, and related civil and criminal legal consequences.

Publicly Available Websites for IT Lawyers

Following are some publicly available websites relating to varying aspects of information technology law practice. Some of these websites may require payment for certain services. Neither the State Bar of Michigan nor the IT Law Section endorses these websites, the providers of the website, or the goods or services offered in connection therewith. Rather these websites are provided for information purposes only and as possible useful tools for your law practice.

Please provide any feedback or recommendations for additional websites to *michael@gallo.us.com*.

Legal Blogs

- *http://thettablog.blogspot.com* – Comprehensive and authoritative discussion of Trademark Trial and Appeal Board proceedings.
- *http://www.thecorporatecounsel.net/blog/index.html* - A great and timely source for finding out what is going on with the Securities and Exchange Commission and the federal securities laws.
- *http://www.chinalawblog.com* – Influential blog on China law for business.
- *http://www.iphonejd.com* – Lawyers using iPhones and iPads.
- *http://bowtielaw.wordpress.com* – The knotty issues of e-Discovery.
- *http://www.lawsitesblog.com* – Tracking new and intriguing web sites for legal professionals.

SBM Practice Management Resource Center's "Order in the Court: Trial by iPad" Seminar Set for June 18 in Lansing

The use of innovative technology in the courtroom will be highlighted at an interactive seminar in Lansing on June 18. Organized by the State Bar of Michigan's Practice Management Resource Center, "Order in the Court: Trial by iPad" will be held from 8:30 a.m. to 4:15 p.m. at the Lansing Community College West Campus Auditorium at 5708 Cornerstone Drive.

Speakers will show attorneys how to incorporate technology into everyday practice and the courtroom and the advantages of doing so. Topics include: "From Discovery to Verdict: Building your Case for Trial Using the iPad;" "Preppin' the iPad for Trial: Moving Documents, Managing Transcripts, and Tracking Jurors;" and "Presenting from the iPad: Hardware, Power Points, and other Trial Presentation Apps." Attorneys who own iPads are encouraged to bring them along.

The Hon. David McKeague, of the U.S. Court of Appeals for the Sixth Circuit, will speak on the logistics of presenting a case electronically. Judicial expectations of trial lawyers using courtroom equipment will be addressed, including suggestions on how to present, authenticate, and publish electronic exhibits to the jury.

It is not necessary to own an iPad to attend the seminar, which costs $95. To register for the seminar, visit *http://www.michbar.org/pmrc/TrialIPAD.cfm*. For more information, contact SBM Practice Management Advisor JoAnn Hathaway at *jhathaway@mail.michbar.org* or (517) 346-6381.