



E-DISCOVERY UPDATE

E-Discovery Task Force Update

The legal framework in litigation for addressing the explosion in electronic communications has been in flux for a number of years. Sidley Austin LLP has established an "E-Discovery Task Force" to stay abreast of and advise clients on this shifting legal landscape. An inter-disciplinary group of more than 25 lawyers across all our domestic offices, the Task Force monitors and examines issues and developments in the law regarding electronic discovery. The Task Force works seamlessly with our firm's Litigators who regularly defend and prosecute all types of litigation matters in trial and appellate courts, federal and state agencies, arbitrations, and mediations throughout the country. The co-chairs of the E-Discovery Task Force are:

Alan C. Geolot
+1 202.736.8250
ageolot@sidley.com

Colleen M. Kenney
+1 312.853.4166
ckenney@sidley.com

Joel M. Mitnick
+1 212.839.5871
jmitnick@sidley.com

To receive future copies of this and
other Sidley Updates via email,
please sign up at
www.sidley.com/subscribe

Attorney Advertising - For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000. Prior results do not guarantee a similar outcome.

Notable E-Discovery Cases and Events

This update addresses the following recent events and court decisions involving e-discovery issues:

1. The Phase One Report of the Seventh Circuit's Electronic Discovery Pilot Program Committee finding that the bench and bar have on a preliminary basis reacted favorably to the Principles Relating to the Discovery of Electronically Stored Information established in connection with the Pilot Program;
2. A May 28, 2010 order by Judge Shira Scheindlin revising her decision in *Pension Comm. of U. of Montreal Pension Plan v. Banc of America Securities, LLC*, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010);
3. A California District Court decision finding that social networking sites such as MySpace and Facebook fall within the ambit of the Stored Communications Act and that private email sent using Facebook and MySpace messaging services may not be disclosed by the provider pursuant to a civil discovery request;
4. A decision from the Southern District of New York finding defendants to be grossly negligent for, *inter alia*, failing to implement a written litigation hold, allowing relevant documents to be destroyed, failing to produce relevant documents, and failing to investigate plaintiff's claims regarding defendants' inadequate document productions; and
5. A Southern District of New York decision ordering defendant to pay \$10,000 in monetary sanctions for spoliating relevant evidence but rejecting plaintiff's claim that defendant had committed a fraud on the court, which defendant rebutted in part by alleging that plaintiff had engaged in "IP spoofing" to make it appear that defendant had sent anonymous derogatory emails to plaintiff.

This **Sidley Update** has been prepared by Sidley Austin LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

1. On May 3, 2010, the Seventh Circuit's Electronic Discovery Pilot Program Committee presented its paper on the Pilot Program's recently completed Phase One (the "Phase One Report") to the Seventh Circuit Bar Association and reported generally positive reactions by the bench and bar to the "Principles Relating to the Discovery of Electronically Stored Information" (the "Principles").

Pilot Program Overview. The Pilot Program was initiated in May 2009 to provide guidance to courts in the Seventh Circuit in their management of the pretrial discovery process in order to make that process, particularly as it relates to e-discovery, more streamlined and less expensive. In September 2009, the Pilot Program Committee adopted the Principles, which encourage cooperation, proportionality, and early discussion and resolution of disputes with respect to ESI-related issues, with potential consequences such as waiver of issues and sanctions for failure to comply. Among other things, the Principles strengthen, and provide further guidance regarding, the meet-and-confer process; encourage and, as to any dispute brought to the court, require the involvement of an "e-discovery liaison" to facilitate discussions between the parties; and provide guidance regarding the scope of document preservation as well as guidance for the use of preservation requests and responses designed to make such devices, when used, productive.

Phase One Results. Phase One of the Program ran from October 2009 through March 2010. During that time, 13 judges of the U.S. District Court for the Northern District of Illinois implemented the Principles through entry of a standing order in 93 civil cases pending on their individual dockets. In March 2010, survey questionnaires were sent to all judges and attorneys involved in the Phase One cases. Responses were received from all 13 judges and from 46% (133 of 285) of attorneys. Although the limited duration and number of cases involved in Phase One caution against extrapolation of the survey results, the Committee believes that those results nevertheless are valuable as a "preliminary, anecdotal 'snapshot' of the information gathered regarding the application of the Principles in cases during Phase One." Phase One Report at 1.

The Phase One Report indicates that overall, survey responses from both judges and attorneys were supportive of the Principles. Although many responses indicated that it was too early to tell whether certain of the individual Principles were effective, 100% of judges either "agreed" or "strongly agreed" that the involvement of e-discovery liaisons contributed to a more efficient discovery process; 90% of judges thought that the Principles "increased" or "greatly increased" counsels' level of attention to the technologies affecting the discovery process and the demonstrated familiarity counsel had with their clients' electronic data and data systems; and 92% of judges agreed that the Principles had a positive effect on counsels' ability to resolve discovery disputes before requesting court involvement. *Id.* at 2. Among attorneys, 43% reported that the Principles "increased" or "greatly increased" the fairness of the discovery process, with most others reporting no effect; 38% reported that the Principles increased the parties' ability to resolve e-discovery disputes without court involvement, again with most others reporting no effect. *Id.* at 2-3. And, particularly encouraging given the Principles' emphasis on cooperation and proportionality, when asked whether application of the Principles affected their ability zealously to represent their clients, 74% of responding attorneys reported "no effect," 22% indicated that the Principles actually *increased* their ability zealously to represent their clients, and only 4% reported that the Principles decreased that ability. *Id.* at 3.

Phase Two and Beyond. The Pilot Program Committee is currently reviewing the Phase One survey results and other feedback from Phase One and is considering whether and to what extent the Principles should be refined for Phase Two of the Program. Phase Two is scheduled to run from July 1, 2010 through May 1, 2011, at which point the Committee will again survey participants and revisit the Principles in anticipation of Phase Three (currently, the last planned test period), which is scheduled to run from July 1, 2011 through May 1, 2012. As part of Phase Two, the Committee expects to increase the number of cases and participating judges, as well as to expand the geographic reach of the Program to include other district courts throughout the Seventh Circuit. By involving more

cases, judges, and courts over a longer period of time, the Principles will be tested more comprehensively in Phase Two than in Phase One, with more meaningful feedback then available to inform the move from Phase Two to Phase Three.

Finally, although at the moment the Pilot Program remains a Seventh Circuit initiative, the program has attracted a considerable amount of interest from courts and practitioners in jurisdictions around the country, causing some observers to expect that over time—potentially, even before the Seventh Circuit has completed all three of its testing phases—similar efforts are likely to emerge elsewhere. Furthermore, given the general utility of the principles and the availability of the standing order by which they are implemented within the Seventh Circuit, litigants in other jurisdictions can always consider moving their own courts to apply the Principles to individual matters through entry of appropriate case management orders.

The full version of the Phase One Report, as well as other materials related to the Pilot Program, can be found at www.7thcircuitbar.org.

2. On May 28, 2010, Judge Shira Scheindlin entered an order in *Pension Comm. of U. of Montreal Pension Plan v. Banc of America Securities, LLC*, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010) amending the language of the opinion to remove a sentence stating that the failure to obtain records from all employees with knowledge of a litigation’s issues was likely to be negligent (as opposed to a higher degree of culpability) and replacing it with a sentence indicating that such conduct *could* constitute negligence.

The following sentence was deleted:

“By contrast, the failure to obtain records from *all* employees (some of whom may have had only a passing encounter with the issues in the litigation), as opposed to key players, likely constitutes negligence as opposed to a higher degree of culpability” 2010 WL at *3 (emphasis in original).

and was replaced with the following:

“By contrast, the failure to obtain records from all those employees who had any involvement with the issues raised in the litigation or anticipated litigation, as opposed to just the key players, could constitute negligence.”

The *Pension Committee* case has been criticized by some for seeking to establish document preservation standards that are too stringent.

3. In *Crispin v. Audigier*, 2010 WL 2293238 (S.D. Ca. May 26, 2010), U.S. District Judge Margaret Morrow addressed whether social networking sites fell within the ambit of the Stored Communications Act (“SCA”). After a lengthy review of the case law, the Court held that private email sent using Facebook and MySpace messaging services was subject to the protection of the Stored Communications Act and may not be disclosed by the provider pursuant to a civil discovery request. The Court further held that Facebook wall postings and MySpace comments also fell under the protective umbrella of the SCA, but only to the extent that these communications were kept private and not made available to the general public.

In this breach of contract and copyright dispute, the plaintiff accused the defendants of violating an oral agreement to use certain of his artwork on clothing manufactured and sold by the defendants. *Id.* at *1. During discovery, the defendants served third-party subpoenas on Facebook, MySpace, Inc. (“MySpace”) and Media Temple, Inc. (“Media Temple”), seeking the plaintiff’s subscriber information as well as certain of the plaintiff’s communications in their possession, such as email messages and wall postings. *Id.* The plaintiff filed an *ex parte* motion to quash the subpoenas arguing, in part, that Facebook, MySpace and Media Temple were prohibited from making such disclosures under the SCA. *Id.*

Stored Communications Act. The SCA places restrictions on communication service providers regarding disclosure of private information about their users. According to the Court, the SCA creates “Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users’ private

information.” *Id.* at *3 (quoting Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 Geo. Wash. L. Rev., 1208, 1213 (2004)). Specifically, it limits the government’s right to compel internet service providers to disclose certain information about their customers and conversely limits the right of those providers to voluntarily disclose the same. *Crispin* at *3.

The statute identifies two categories of communications service providers covered under the SCA: 1) electronic communication service providers (“ECS providers”), defined as “any service which provides to [its] users . . . the ability to send or receive wire or electronic communications,” and 2) remote computing service providers (“RCS providers”), defined as the provision of “computer storage or processing services by means of an electronic communications system.” Stored Communications Act, 18 U.S.C. §2510(15), §2711(2). The SCA prevents ECS providers from divulging the contents of a communication while in “electronic storage” by that service, and prohibits RCS providers from divulging the contents of any communication “carried” or “maintained” on that service. See 18 U.S.C. §2702(a). A central issue in this case was whether Facebook, MySpace, or Media Temple met the definition of an ECS or RCS provider, and if so, whether the information requested constituted protected communications under the SCA.

These matters initially came before Magistrate Judge McDermott, who upheld the third-party subpoena. *Crispin* at *2. The Magistrate Judge held that 1) the SCA did not prohibit disclosure pursuant to a civil subpoena, 2) the SCA did not apply to Facebook, MySpace and Media Temple because they were not ECS providers as defined by the statute and 3) the information sought was not in “electronic storage” and therefore not entitled to the protection for the SCA. *Id.* Upon appeal by the plaintiff, the District Court granted review of the Magistrate Judge’s order, reversing in part and vacating in part.

Standing to Challenge the Subpoena. Judge Morrow first held that the plaintiff had standing to challenge the third-party subpoena because he had a “personal interest” in the information being sought. *Id.* at *5. The Court

specifically observed that “an individual has a personal right in information in his or her profile and inbox on a social networking site and his or her webmail inbox in the same way that an individual has a personal right in employment and bank records.” *Id.* at *5.

Disclosure Pursuant to Civil Subpoena. The Court next found that the SCA prohibits disclosure of information pursuant to a civil subpoena. *Id.* at *6-7. The Court noted that the SCA includes a complex regulatory scheme under which governmental entities can compel production of information protected by the SCA, but only in criminal matters and under limited circumstances. *Id.* at *6. The SCA, however, contains no provisions allowing for disclosure of protected communications pursuant to civil discovery requests, indicating the drafters did not intend for such disclosure. *Id.* The Court further observed:

“Among the Act’s most significant, although unstated, privacy protections is the ability to prevent a third party from using a subpoena in a civil case to get a user’s stored communications or data directly from an ECS or RCS provider.” *Id.* at *7 (quoting Jeremy Robison, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1195, 1208-09 (2010)).

The Court concluded that if information was protected under the SCA, the service provider may not be compelled to disclose that information pursuant to a civil discovery request.

Communication Service Providers. The Court next considered whether Facebook, MySpace or Media Temple met the definition of an ECS or RCA provider under the statute. In conducting this analysis, the Court noted that the SCA was written prior to the advent of the internet and as such was “ill-suited to address modern forms of communication like [Facebook and MySpace].” *Id.* at *14 (quoting *Konop v. Hawaiian Airlines Inc.*, 302 F.3d 868, 874 (9th Cir. 2002)).

The Court first concluded that all three entities qualified as ECS providers because each service provider offered private messaging or email services as part of their accounts. Media Temple, for example, provides “webmail” that allows customers

to view and read email messages from a web-based portal, and Facebook and MySpace also offer private messaging services to their users. *Id.* at *8-9. In reaching this conclusion, the Court relied on what it characterized as the “voluminous” case law that establishes that private messaging or email services qualify as ECS providers. *Id.* at *9.

The Court next observed that “precedent and legislative history establish that the SCA’s definition of an ECS provider was intended to reach a private [bulletin board service].” *Id.* The Court concluded that the Facebook wall and MySpace comments features, which allow messages and comments to be posted and viewed on each user’s page, are the functional equivalent of electronic bulletin board services. *Id.* at *10. The Court emphasized, however, that only providers of secure or restricted electronic bulletin boards, as opposed to public bulletin boards, came under the ambit of the SCA – communications posted on publically available bulletin boards were not intended for protection. *Id.* Here, the Court noted that Facebook and MySpace both provide security setting allowing messages to be viewed only by those granted access to the user’s profile, the use of which would make such bulletin boards private and secure. *Id.*

Having concluded that the three service providers were communication service providers under the SCA, the Court went on to analyze whether the information sought by the subpoena, the private messages and wall postings, constituted protected communications under the SCA. As mentioned above, an ECS provider is prohibited from divulging contents of electronic communication “while in electronic storage by that server.” See 18 U.S.C. §2702(a)(1). Under the SCA, “electronic storage” is defined in two ways. First, it is defined as “any temporary or immediate storage of a wire or electronic communication incidental to the electronic transmission thereof.” 18 U.S.C. §2510(17)(A). This definition has previously been held to include email messages stored on an internet service provider’s server pending delivery to the recipient. *Crispin* at *10. A second definition of “electronic storage” under the SCA is electronic storage “for purposes of backup protection of communications.” 18 U.S.C. §2510(17)(B).

The Court concluded that email messages in the possession of Facebook, MySpace and Media Temple that were delivered to the plaintiff’s inbox but not yet opened by the plaintiff fell within the definition of “electronic storage” because the messages were in “temporary and immediate storage” by the service provider pending delivery to the plaintiff. *Crispin*, at *13. Accordingly, the unread email messages were protected from disclosure under the SCA. *Id.* As to messages that had been opened by the plaintiff and stored in his Facebook, MySpace, or Media Temple inboxes, the Court acknowledged that such messages were no longer in “temporary” storage, but found that at the moment the plaintiff opened and retained a message in his inbox, the service providers went from being an ECS provider to an RCS provider (provider of computer storage and processing services). *Id.* As such, the messages remained protected from disclosure under the SCA. *Id.* On this basis, the Court overruled the Magistrate Judge’s order, and quashed the third-party subpoena to the extent that it sought the contents of plaintiff’s email messages in the possession of Media Temple, Facebook or MySpace. *Id.* at *16.

Turning to the plaintiff’s Facebook wall postings and MySpace comments, the Court reiterated its earlier conclusion that Facebook and MySpace were ECS providers with respect to these private electronic bulletin board features. *Id.* at *14. It further concluded that the communications posted on the wall and comments page were communications in “electronic storage,” because they were maintained by Facebook and MySpace for “backup purposes.” *Id.* In the alternative, the Court concluded that Facebook and MySpace were also RCS providers with respect to the bulletin board features of Facebook and MySpace in that they provided “storage services” for the messages posted on each user’s webpage. *Id.* at *15. Under either theory, the Court concluded that the contents of the plaintiff’s Facebook wall and MySpace comments were protected from disclosure under the SCA, but only to the extent that the wall postings and messages were privately maintained. *Id.* The Court held that there was insufficient evidence in the record to determine whether the plaintiff took advantage of the security protocols offered by Facebook and MySpace and protected their wall and comment

communications from general view. *Id.* Accordingly, the Court vacated Magistrate Judge McDermott's order upholding the subpoena relative to these communications and remanded it for further evidentiary review of the outstanding privacy questions. *Id.*

4. In *Merck Eprova AG v. Gnosis S.p.A, et al.*, 2010 WL 1631519 (S.D.N.Y. April 20, 2010), the Court awarded Merck costs, including attorney's fees, and additionally sanctioned defendant Gnosis with a \$25,000 fine for failing to produce documents that should have been provided in discovery.

In this case, brought under the Lanham Act, plaintiff raised repeated questions regarding the completeness of defendants' document response and initial disclosures. Over a period of several months, defendants slowly provided additional documents in response to the complaints, but each time "failed to ... remedy ... deficiencies." *Id.* at *2. The dispute resulted in a phone conference with U.S. District Judge Richard Sullivan in which the judge found defendants' production incomplete and ordered defendants to complete their disclosures. In response, defendants produced additional materials, but even these productions did not "remedy ... deficiencies" noted months earlier. *Id.* Plaintiff alleged that the omission of certain documents—which defendants stated had been produced—was intentional. Defendants "dismissed as absurd the possibility that the documents were missing from the [production] e-mail and CD." *Id.* After an evidentiary hearing, the Court found that defendants had in fact failed to produce certain documents—but those failures appeared to be inadvertent. Defendants, however, had represented multiple times to the Court that plaintiff's discovery claims were false, but "never actually investigated their validity." *Id.* Even after defendants discovered that their statements to the Court were false, they produced all the documents to plaintiff but waited a month to correct their statements to the Court.

A subsequent evidentiary hearing on the issue "shed little light on the conflict over the ... disclosures, [but] ... did reveal several troubling details about Defendants' behavior during the course of discovery, thereby partially explaining why [Defendants'] production had been intermittent and

incomplete." *Id.* at *3. In particular, the Court found that (1) defendants had not issued a litigation hold—oral or written, (2) defendants continued deleting emails and/or prevent automatic deletion of emails after the litigation began, (3) defendants failed to produce admittedly responsive documents because they deemed them "insufficiently material" and (4) defendants chose not to spend too many resources on the litigation because it related to a small portion of their business. *Id.* Defendants also appeared to engage in witness coaching during a deposition of one of their expert witnesses by passing notes.

Citing *Pension Committee*, Judge Sullivan held that defendants' failure to issue any sort of litigation hold constituted gross negligence and therefore there was "no reason to make further findings with regard to whether other aspects of Defendants' conduct would be independently sanctionable." *Id.* at *5. The Court did note, however, that defendants' conduct "far exceeded the bounds of acceptable behavior" when they did not exercise diligence in conducting the searches, coached deponents, chose not to produce responsive documents, and failed to investigate plaintiff's inquiries about their document productions. *Id.* The Court ordered that plaintiffs pay costs, including attorney's fees, related to the production issues and fined plaintiffs \$25,000. The Court did not apportion liability between defendants and defense counsel "under the belief that they are best suited to make that decision, and out of a concern [regarding protection of] attorney-client confidentiality." *Id.* at *6. The Court deferred making until a future date a decision on whether an adverse jury instruction would be appropriate.

5. In *Paslogix, Inc. v. 2FA Technology, LLC*, 2010 WL 1702216 (S.D.N.Y. April 27, 2010), the Court ordered that defendant 2FA Technology pay \$10,000 in monetary sanctions for spoliating relevant emails, computer logs, and Skype messages but declined to grant other more severe sanctions sought by plaintiff. The Court also found that defendant's affirmative defense of "IP spoofing," in addition to other proffered evidence, sufficiently rebutted plaintiff's allegations that defendant had committed fraud on the court.

During the course of discovery in this breach of a licensing agreement case, plaintiff raised a “fraud on the court” allegation against defendant, asserting that one of defendant’s employees had sent an anonymous email in an effort to expand discovery, cause competitive harm, and garner a favorable settlement. The case presents two main e-discovery issues: “IP spoofing” and spoliation of evidence.

IP Spoofing. During the course of litigation, plaintiff received several anonymous emails from hushmail.com addresses. These emails essentially cast aspersions on plaintiff which, if true, would benefit defendant in the litigation (who had filed counterclaims) and potentially expand discovery. For example, in one email the author wrote that plaintiff’s actions essentially killed [defendant’s] opportunity to get a Wal-Mart deal. *Id.* at *2. After receiving these emails, plaintiffs engaged counsel to conduct an internal investigation and ultimately traced the emails back to IP addresses linked with one of defendant’s officers and his wife. In response to plaintiff’s allegations regarding the anonymous emails, defendant raised the defense of IP spoofing. IP spoofing is “a practice whereby a person can make his true IP address appear to be any address he chooses.” *Id.* at *4.

Defendant argued that a “Passlogix employee may have ‘spoofed’ his IP address in an effort to impersonate [the defendant] on the Internet.” *Id.* Because defendant was an expert in IT security, he stated that if had he sent the emails, his knowledge and expertise would have allowed him to ensure that no emails could have been traced back to him. Moreover, he offered various reasons, including grammatical/spelling features of the emails, that suggested he could not have written them. In one of those Perry Mason moments, a former

employee of plaintiff in fact confessed under oath to having spoofed defendant’s IP address.

The Court held extensive evidentiary hearings on the IP spoofing issues and heard testimony from expert witnesses on this complex and technologically advanced area of internet communications. *Id.* at *6–8. Ultimately, after a thorough review of the evidence presented by both sides, the Court held that plaintiff failed to prove by clear and convincing evidence that defendant committed fraud on the court. *Id.* at *10–21.

Spoliation. With respect to the issue of spoliation, the Court did find that the defendant “was on notice that some of his written communications . . . were probative of the underlying litigation when the communications were deleted” and that defendant’s “failure to preserve these written communications, in addition to 2FA’s overall failure to issue a written litigation hold notice, constitutes gross negligence.” *Id.* at *31–32. Accordingly, the Court found that defendants “engaged in spoliation of evidence,” including emails, text-messages, and Skype messages. *Id.*

Despite plaintiff’s requests for more severe sanctions, including adverse inferences and exclusion of evidence, the Court held that a monetary fine of \$10,000 against 2FA best suits “the facts and evidentiary posture of [this] case.” *Id.* at *37 (citation omitted). The Court noted:

“Here, a fine against 2FA serves the dual purposes of deterrence and punishment. . . . Because Salyards and Cuttill are the sole principals of 2FA, a fine directed at 2FA will affect them directly. In concluding that a fine of \$10,000 is the most appropriate sanction, the Court balances 2FA’s litigation conduct with its status as a small corporation.” *Id.*

If you have questions about any of these items, please contact your regular Sidley Austin LLP contact.

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

www.sidley.com

Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm’s offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley, or the firm.

SIDLEY AUSTIN LLP
SIDLEY