



E-DISCOVERY UPDATE

October Edition of Notable Cases and Events in E-Discovery

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

1. A Maryland federal court decision by Magistrate Judge Paul Grimm upholding against a privacy challenge a third party subpoena for a party's cell phone text messages, telephone bills, and incoming and outgoing call records;
2. A decision by a District of Columbia federal court finding that privilege had been waived with respect to an inadvertently produced attorney-client communication because the defendant failed to take reasonable steps to prevent disclosure of the communication or to rectify the disclosure once discovered;
3. A Virginia federal case rejecting claims of undue burden and expense and requiring production and restoration of backup tapes for review of potentially relevant emails relating to fraud and discrimination claims; and
4. A California federal court ruling that certain emails were inadmissible because the plaintiff could not authenticate the emails and establish that the purported author of the emails in fact wrote or sent them.

1. In *Corsair Special Situations Fund, L.P., v. Engineered Framing Systems, Inc.*, 2011 WL 3651821 (D.Md. Aug. 17, 2011), Magistrate Judge Paul Grimm upheld a third party subpoena request for defendant's cell phone text messages, telephone bills, and incoming and outgoing call records, despite defendant's claim that release of that information would violate her right to privacy.

In seeking to collect on a judgment obtained against defendant, plaintiff served a subpoena on Verizon Wireless, seeking, *inter alia*, all text messages sent or received from the defendant's cell phone as well as invoices, telephone bills, and incoming and outgoing phone call records. Magistrate Judge Grimm stated that a party had standing to challenge a third party subpoena only if the party "claims some personal right or privilege in the information sought by the subpoena." *Id.* at *2 (internal citations and quotations omitted). The defendant moved to quash the subpoena, claiming that production of such records would violate her right to privacy. *Id.* at *1.

Magistrate Judge Grimm denied the defendant's motion, ruling that the defendant had failed to demonstrate she had standing to challenge the subpoena. He noted the lack of specificity in defendant's motion and what he referred to as her "vaguely" asserted right to privacy. *Id.* at *2. He observed that she had failed to point to any "supporting authority" or cite to any applicable Fourth Circuit case law "holding that a party has a protected privacy interest in the contents of text messages that the party sent or received." *Id.* at *3.

Magistrate Judge Grimm noted that there is no consistency in the other circuits on the issue of the privacy of the contents of text messages. In *United States v. Finley*, the Fifth Circuit held that a defendant had a reasonable expectation

of privacy in text messages sent from his cell phone. 477 F. 3d 250, 259 (5th Cir. 2007). The Eleventh Circuit, however, concluded a defendant did not. *United States v. Jones*, 149 Fed. App'x 954, 959 (11th Cir. 2005). In *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010), the only case in which the Supreme Court has considered the issue, the Court did not resolve the parties' dispute over whether the defendant had a reasonable expectation of privacy in his text messages. In side-stepping the question, the Court stated in part, "[t]he Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *Id.* at 2629.

With respect to the telephone bills and invoices, Magistrate Judge Grimm drew an analogy to bank transaction records, which are treated as business records, and not as a customer's private information. *Corsair*, 2011 WL 3651821, at *3. He concluded that phone company records are business records and not personal documents in which a customer has a reasonable expectation of privacy. Having reached this conclusion, Magistrate Judge Grimm concluded that the defendant did not have standing to challenge the subpoena.

Noting the unsettled nature of the law in this area, Magistrate Judge Grimm ruled that the subpoenaed information would be subject to a protective order limiting use of the information to assisting with collection of the judgment, prohibiting the copying or dissemination of the information beyond what was necessary to accomplish that goal, and requiring the return or destruction of the information once the judgment was satisfied. *Id.* at *4.

2. In *Williams v. District of Columbia*, 2011 WL 3659308 (D.D.C. Aug. 17, 2011) the Court denied a motion to exclude introduction of an inadvertently produced privileged communication, holding that the privilege had been waived because the defendant failed to take reasonable steps to prevent disclosure of the communication or to rectify the disclosure once discovered.

In a suit brought against the District of Columbia (the District) under the District's Whistleblower Protection Act, the District inadvertently produced a communication from one of its attorneys discussing the plaintiff's termination. *Id.* at *1. When the District realized its error, it contacted the plaintiff and requested that the communication be returned and that the plaintiff refrain from using or disclosing the information contained therein. *Id.* The Plaintiff never responded to the notice, and the District never followed up on the matter. Nearly two and a half years later, after the plaintiff listed the communication on her exhibit list for trial, the District brought a motion to exclude the communication, arguing it was privileged and had been inadvertently disclosed during discovery. *Id.* at *2. The Court denied the District's motion.

U. S. District Judge Colleen Kollar-Kotelly began her analysis by reviewing the provisions of Federal Rule of Evidence 502(b). *Id.* at *2-3. Under that provision, disclosure of documents covered by the attorney-client privilege does not constitute a waiver of the privilege if: (1) the disclosure was inadvertent, (2) the holder of the privilege took "reasonable steps" to prevent disclosure, and (3) the holder "promptly took reasonable steps to rectify the error." *Id.* at *3 (quoting Fed. R. Evid. 502(b)). The Court held that the District failed to demonstrate both that it took "reasonable steps" to prevent disclosure or that it "promptly took reasonable steps to rectify the error." *Id.*

To demonstrate that it had taken "reasonable steps" to prevent disclosure, the District submitted an unsworn averment of its counsel stating that the documents had been reviewed by an "experienced" paralegal under the supervision of an attorney. *Id.* at *3-4. The averment, however, was made by counsel who had not been involved in the case at the time of the review, and the averment failed to provide any detail on exactly how the review was conducted, such as how much time was spent on the review, the exact nature of the paralegal's "experience," how many rounds of review were conducted, or the total number of documents that were reviewed and produced. *Id.* at *3-4. The Court characterized the District's submission as "uninformative" and "so cursory and incomplete that there simply is no foundation for this Court to evaluate the reasonableness of the precautions taken to guard against inadvertent disclosure." *Id.* at *4-5.

On this point, the Court stated:

“It should go without saying that this sort of conclusory statement is patently insufficient to establish that a party has discharged its duty of taking ‘reasonable steps’ to guard against disclosure of privileged documents.” *Id.* at *4.

With respect to the District’s efforts to “promptly” take “reasonable steps to rectify the error,” the Court also found the District fell short. It was not enough that the District notified the defendant of the inadvertent disclosure and asked that the communication be returned. *Id.* at *5. When the defendant failed to respond, the District should have followed up. *Id.* Instead, it waited over two and a half years before it raised this issue again. The Court observed that “[t]his sort of indifference is fundamentally at odds with the principle that the attorney-client privilege ‘must be jealously guarded by the holder of the privilege lest it be waived.’” *Id.* (citation omitted). The Court denied the District’s motion to exclude the communication and ordered the plaintiff to file a notice with the Court explaining on what basis the communication was admissible and how she intended to use it at trial. *Id.* at *6.

3. In *United States v. Universal Health Services, Inc.*, 2001 WL 3426046 (W.D. Va. Aug. 5, 2011), the Magistrate Judge ordered the Commonwealth of Virginia to produce backup tapes for review of potentially relevant email traffic relating to fraud and discrimination claims. The Court rejected claims of undue burden and expense and required production of the tapes to defense counsel to provide to a commercial vendor to retrieve relevant files in a format usable by the Commonwealth to research for responsive documents.

In this discrimination and false claims case, relators claimed that the defendants had submitted fraudulent claims to the Virginia Medicaid program. In the course of discovery, defendants sought to compel production of documents relating to alleged complaints of Medicare fraud made by the relators to the Commonwealth. *Id.* at *1. The Commonwealth originally objected to the requested production from various state agencies, but the Magistrate Judge ordered production by all relevant state agencies. *Id.* On the date set for production, the Commonwealth objected that the production of documents would be unduly burdensome and supported that claim with an affidavit stating that the Department of Behavioral Health and Developmental Services (DBHDS) had switched email systems in 2009 and that emails sent prior to that period were on backup tapes that could not be accessed with the current DBHDS exchange server. The Commonwealth affidavit noted that under state law any backup tape restoration would have to be performed by the Commonwealth’s technology group and estimated the cost at more than \$100,000, but acknowledged that more efficient and less expensive means of restoring the information on the backup tapes did exist. *Id.* at *3. Based on this and related submissions, the Commonwealth argued that it should not be required to search its backup tapes for the responsive documents due to the burden and expense required. The defendants offered their own e-discovery expert who stated that his company could retrieve the information stored on the backup tapes in a cost effective and timely manner using readily available technology, but could not provide an estimate of the time or expense required until he had reviewed the materials.

The Magistrate Judge stated that the party seeking to avoid production must demonstrate that the information sought was “not reasonably accessible because of undue burden or cost.” Fed. R. Civ. P. 26(b)(2)(B). Upon a finding of undue burden or cost, the Court can still order the discovery of the information upon a showing of good cause after taking account of the burden and expense, the likely benefit, the need for the information in the case, the amount in controversy, the parties’ resources, the importance of the issues at stake, and the importance of the discovery in resolving the issues. Fed. R. Civ. P. 26(b)(2)(C).

In this instance, the Magistrate Judge concluded that the Commonwealth had not made the necessary showing of undue burden. The Magistrate Judge noted that the Commonwealth did not put in place a litigation hold until April 2010, even though it knew as of April 2008 that it would intervene in the action and that the DBHDS records would be relevant to the claims. *Id.* at *5. In addition, the defendants had shown that relevant ESI did exist on the DBHDS email systems prior to 2009 in that the relators all claimed that they had sent pre-2009 emails regarding the fraud to

DBHDS. The Magistrate Judge concluded that the ESI had become less accessible based on the Commonwealth's failure to take steps to adequately preserve relevant ESI.

The Magistrate Judge also noted that the Commonwealth was seeking recovery of more than \$10 million on the fraud claim and that the Commonwealth's affidavit had acknowledged that the backup tapes could be restored at less cost using commercial means that did not rely on the Commonwealth's technology group. Finding that the pre-2009 email files likely contained documents relevant to the defense of the case, the Magistrate Judge ordered that the backup tapes containing those pre-2009 email files be produced to defense counsel for use by a commercial vendor to restore the files in a format usable by the Commonwealth to search for responsive documents.

The Magistrate Judge concluded by ruling that the cost of retrieving the pre-2009 emails would be borne initially by the defendants, subject to their filing a motion outlining an estimate of the costs to be incurred and seeking reimbursement from the Commonwealth. *Id.* at *6.

4. In *Jimena v. UBS AG Bank, Inc.*, 2011 WL 2551413 (E.D. Cal. June 27, 2011), the Court ruled that certain emails were inadmissible because the plaintiff could not firmly establish that the author of the emails was the person that the plaintiff claimed it to be.

Plaintiff alleges that he was defrauded when he received emails purportedly from Clive Standish (Standish), then Chief Financial Officer of UBS, offering to transfer \$19 million into plaintiff's bank account from a bank in Nigeria if plaintiff first transferred \$51,000 to an account at another bank. *Id.* at *1. The \$51,000 was allegedly needed to satisfy a non-existent "Anti Drug/Terrorist Clearance" fee required for all money transfers out of Nigeria. *Id.* Plaintiff made the requested transfer but never received the \$19 million. *Id.* Plaintiff's primary evidence that Standish at UBS sent the emails was the email addresses from which the communications came, `clive_standish@yahoo.com` and `customerservices@privateclientsub.cjb.net`, coupled with the fact that the emails were purportedly signed by Standish and contained UBS's phone number and address. *Id.* at *1, 6. Plaintiff brought suit claiming, in part, that UBS was wrongfully in possession of the \$51,000 he had transferred into another bank account and that UBS owed him the promised \$19 million. *Id.* UBS filed for summary judgment, arguing that the emails were inadmissible unauthenticated hearsay without which the plaintiff would be unable prove his claim. *Id.* at 2. UBS asserted that the Yahoo account could have been created by anyone because Yahoo does not require any proof that the person establishing the email address is the individual named in the email address. UBS further asserted that `www.cjb.net` is a website service that allows users to create an email address of their choosing without requiring proof of the identity of the user establishing the account or evidence that the user works for the associated business. The Court considered the issue of admissibility and agreed with UBS.

When considering a motion for summary judgment, the Court may consider only admissible evidence. *Id.* at *3. Authentication is a "condition precedent" to admissibility. *Id.* at *3 (citing Fed. R. Evid. 901(a)). Authenticity can be satisfied "by evidence sufficient to support a finding that the matter in question is what its proponent claims." *Id.* (citing Fed. R. Evid. 901(a)). The plaintiff attempted to authenticate the emails in two ways: first, through a personal affidavit attesting to the source of the emails; and, second, by relying on the content of the emails themselves. The Court rejected both approaches. The Court held that an affidavit provided by the plaintiff was insufficient authentication because it provided no foundation linking the emails to Standish, the alleged author. *Id.* at *3-4. The plaintiff had provided an affidavit attesting to the source of the emails (he stated that he received the emails through his Yahoo email account, that his account was password protected and secure, and that he printed the emails out directly from his computer). *Id.* at *4. The plaintiff, however, never stated that he had witnessed or otherwise had any direct knowledge that Standish wrote the emails, and plaintiff could not provide any confirmation from Standish that he had written the emails. *Id.* at 4. The plaintiff argued that the content of the Standish emails contained unique identifiers sufficient to establish they had been sent by Standish, including Standish's name, and his address and telephone number at UBS. *Id.* at *5. The Court found this argument unpersuasive. First, while the appearance of UBS's address and telephone number could, under certain circumstances, assist with authentication, here the information was publicly

available to anyone seeking to use it. *Id.* at *6. Second, the email addresses were a product of publicly available email service providers that anyone could have used to establish an account under Standish's name. *Id.* Third, nothing in the substance of the email communication confirmed Standish as the author. *Id.*

In comparing the email to the receipt of an unsolicited letter, the Court stated:

“When a letter, signed with the purported signature of X, is received ‘out of the blue,’ with no previous correspondence, the traditional ‘show me’ skepticism of the common law prevails, and the purported signature is not sufficient as authentication, unless authenticity is confirmed by additional facts.” *Id.* at * 6 (quoting vol. 2 Kenneth S. Broun, McCormick on Evidence § 224 (6th ed. 2006)).

The Court concluded that the Standish emails were “unsolicited, contain[ed] only publicly available, self-serving information, and [did] not contain any substantive or unique information that supports authenticity.” *Id.* at *7. The Court also held that the emails were hearsay and not admissible under any exception, including the exception for admission of a party-opponent. Under the Federal Rules of Evidence, a statement is not hearsay if offered against a party and it is the “party’s own statement, in either an individual or representative capacity.” Fed. R. Evid. 801(d)(2)(D). Because there was insufficient evidence that the emails were written or sent by Standish, the statements did not constitute party-opponent admissions. *Id.* at *8.

Finding that the emails were inadmissible, the Court held there was “an absence of admissible evidence to create a triable issue of material fact” and granted UBS’s motion for summary judgment. *Id.* at *8.

If you have any questions regarding this update, please contact the Sidley lawyer with whom you usually work.

The E-Discovery Task Force of Sidley Austin LLP

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 interdisciplinary 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

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