



## E-DISCOVERY UPDATE

### November Edition of Notable Cases and Events in E-Discovery

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

1. A California federal court decision enforcing an SEC subpoena requiring an Internet service provider to turn over identifying information regarding the owner of an email account and rejecting the owner's claim that such action would violate his right to free anonymous speech;
2. A New York federal Magistrate Judge granting criminal defendants' motions to compel and ordering the prosecution to produce electronically stored criminal discovery in a format suitable for searching or in native format;
3. A Northern District of Illinois decision finding that the defendant waived attorney-client privilege with respect to privileged documents inadvertently posted to a production website accessible by the plaintiff; and
4. A New Jersey district court decision finding spoliation of evidence and ordering defendant to briefly change his Facebook profile picture to include a prior photograph to allow plaintiff to print Facebook pages as they had existed prior to changes made by defendant.

**1. In *Doe v. Securities and Exchange Commission*, 2011 WL 4593181 (N.D. Cal. Oct. 4, 2011), United States Magistrate Judge Nandor J. Vadas upheld an SEC subpoena compelling Google, Inc. to turn over identifying information regarding the owner of a certain email account, despite the owner's claim that such action would violate his right to free anonymous speech.**

Under its investigative powers, and pursuant to the Electronic Communications Privacy Act (ECPA), the SEC issued a subpoena to Google requesting the identity and contact information for the owner of aurorapartners@gmail.com. *Id.* at \*1. The SEC issued the subpoena in connection with the investigation of a so-called "pump and dump" scheme related to Jammin Java Corporation. *Id.* "Pump and dump" is a scheme in which a stock owner attempts to artificially inflate the price of the stock through false or misleading statements with the intent to profit by then selling the stock after the price appreciation. The SEC was investigating whether false or misleading statements were made in certain online newsletters prior to a rapid increase in Jammin Java's stock and, if so, whether the authors of the online newsletters failed to disclose a financial interest or tie to the company. *Id.* The SEC claimed it had evidence that the email address was associated with the websites on which the newsletters were published. *Id.* at \*5. Upon receipt of the subpoena, Google notified the owner who, in turn, sought to quash the subpoena. *Id.* at \*1. The movant argued that disclosure of his identity would violate his right to anonymous speech because he used the email address "to speak anonymously on the Internet" and "post my opinion on various political blogs." *Id.* at \*2.

The ECPA requires that providers of electronic communication services, such as Google, provide certain information about its customers, including name, address, and contact phone number, when served with an administrative subpoena. 18 U.S.C. § 2703(c)(2). The standard of review in an agency subpoena enforcement proceeding in the Ninth Circuit is governed by the three-part *Brock* test: “(1) has Congress granted the agency the authority to investigate; (2) have procedural requirements been followed; and (3) is the information sought relevant and material to the investigation.” *Doe*, 2011 WL 4593181, at \*3 (citing *Brock v. Local 375, Plumbers Int’l Union of America*, 860 F.2d 346, 348 (9th Cir. 1998)). Under *Brock*, if a party opposing disclosure makes a prima facie showing of a first amendment issue, the burden shifts to the government to show that the “information sought is rationally related to a compelling governmental interest” and that the subpoena is the “least restrictive” way of retrieving the information. *Doe*, 2011 WL 4593181, at \*3. The movant claimed that a more rigorous test than *Brock* should govern the dispute and argued that the SEC was required to notify him of the subpoena, produce prima facie evidence supporting the elements of its claim, and demonstrate the relevancy of the information sought to the legal claims made. At that point, the Court would balance the interests of the parties. *Id.*

Magistrate Judge Vadas declined to apply the more rigorous test proposed by the movant, noting that the movant was relying on civil discovery cases, rather than agency subpoena cases, in arguing for a more rigorous test. The Magistrate Judge also found that “Congress recognize[d] the need for government agencies to investigate wrongdoing and accordingly has granted these agencies investigatory powers that are not available to civil parties.” *Id.*

Magistrate Judge Vadas concluded that the SEC had met all three prongs of the *Brock* test: first, Congress expressly granted the SEC the authority to investigate potential violations of securities laws, *id.* at \*5; second, the SEC followed the proper procedures for serving the subpoena—under the ECPA, the SEC is not required to notify the customer of a request for his or her records, *id.*; and third, the information sought was relevant and material to the SEC’s investigation. *Id.* An agency subpoena will “survive a relevancy challenge as long as the information requested touches a matter under investigation.” *Id.* at \*6 (internal quotation omitted). The SEC had declared under penalty of perjury that it “obtained information indicating that the email address [ ] potentially belongs to a touter in the “pump and dump” scheme.” *Id.* at \*5 (citation omitted). Magistrate Judge Vadas held that the SEC was not required to support this statement with admissible evidence, as the movant claimed, or demonstrate that a violation had actually occurred, to survive a relevancy challenge. *Id.* at \*6.

Finally, Magistrate Judge held that the movant failed to make a *prima facie* showing of a first amendment infringement such that the SEC was required to establish a compelling interest in the identity of the email owner. In so ruling, Magistrate Judge Vadas stated, “in the context of valid government investigations, courts repeatedly have concluded that identifying information is not subject to First Amendment (or Fourth Amendment) protection.” *Id.* Magistrate Judge Vadas observed that the movant had freely provided this information to Google when he signed up for the email account, and that disclosure of such information turned over to a third party is “routinely” ordered by the courts. *Id.* at \*3.

## **2. In the criminal case of *United States v. Briggs*, 2011 WL 4017886 (W.D.N.Y. Sept. 8, 2011), United States Magistrate Judge Hugh B. Scott granted defendants’ motions to compel and ordered the prosecution to produce certain electronically stored criminal discovery in a format suitable for searching or in the information’s native format.**

In this case of first impression for the district and circuit, the Magistrate Judge grappled with the issue of whether the prosecution’s production of substantial volumes of electronic discovery in .tiff format was appropriate and how the court should deal with “manner of production” issues in criminal cases. The case arose from an extensive investigation of a drug trafficking ring, during which time the government used “court-authorized interceptions of cellular telephone communication indicating that defendants allegedly engaged in drug trafficking.” *Id.* at \*2. The government produced

audio recordings of these communications as well as other data collected by a system called “VoiceBox.” In particular, data regarding the calls were produced in .tiff format, which was not readily searchable by defendants. *Id.*

In their motion, defendants contended that they wanted the data presented in either its native format or in a “text-accessible PDF” and argued that the government had the ability to produce in those formats. *Id.* The government raised a number of objections, including that there were system limitations to what it could provide and that “the United States Attorney’s Office did not have server space to retain an OCR copy of materials ... and such a duplication is cost-prohibitive.” *Id.* at \*3. Finally, the government contended that it would not produce the documents in native format because it wants to “prevent the disclosure of cooperators which [were] redacted when [produced in .tiff].” *Id.*

The Magistrate Judge spent considerable time addressing the lack of guidance in the criminal rules about the manner of production of criminal discovery. He explained that only a handful of cases have addressed the issue, including *United States v. O’Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008) [in which Sidley served as defense counsel]. The Magistrate Judge quoted the Sixth Circuit as stating that “Federal Rule of Criminal Procedure 16 is ‘entirely silent on the issue of the form that discovery must take,’” (*id.* at \*6 (quoting *U.S. v. Warshak*, 631 F.3d 266, 296 (6th Cir. 2010))), and also noted that “there is scant authority on the manner to which parties are to produce discovery in *criminal* cases.” *Id.* (emphasis in original). Ultimately, however, Magistrate Judge Scott determined that on a case-by-case basis the court had discretion under Fed. R. Crim. P. 16 to direct the manner of production. *Id.* at \*5. He then noted: “The ‘typical’ criminal case usually does not have the volume of documents that was presented either in this case, *O’Keefe*, or *Warshak*. But, as the technology becomes more prevalent, the Government and defendants will come to produce more and more ESI...along with other, traditional forms of discovery.” *Id.* at \*7.

Under this rationale, the Magistrate Judge “determine[d] that **the Government** is the party better able to bear the burden of organizing the[] records for over twenty defendants in a manner useful to all.” *Id.* at \*8 (emphasis in original). He therefore ordered the government “to reproduce its disclosure in a searchable format (PDF, for example) or in native format, indicating the manner of that reproduction.” *Id.* The Magistrate Judge stated that he “need not go as far as the District of District of Columbia in *O’Keefe* and adopt the pertinent Federal Rules of Civil Procedure wholesale as the standard for production of criminal ESI.” *Id.* He did, however, urge the Advisory Committee on Criminal Rules to address this issue.

**3. In *Thorncreek Apartments III, LLC v. Village of Park Forest*, 2011 WL 3489828 (N.D. Ill. Aug. 9, 2011), Magistrate Judge Sidney Schenkier held that the defendant waived the attorney-client privilege with respect to certain documents designated as privileged that were inadvertently posted onto a production website accessible by the plaintiff.**

The dispute arose after what appears to have been a miscommunication between the defendant and the vendor it used to produce its documents. In response to discovery requests from the plaintiff, the defendant had conducted a review of over 250,000 pages of electronic documents. *Id.* at \*7. According to the defendant, an attorney reviewed each document and designated it with one of three tags: responsive, non-responsive, or privileged. *Id.* at \*1. The defendant intended to post only two types of documents onto the production website: responsive documents and non-responsive documents. The non-responsive documents were produced to “show the [plaintiff] how many non-responsive documents had been identified in the review.” *Id.* The privileged documents were intended to be withheld from the production. *Id.* at \*7. The review took place over a period of about six months, with rolling productions beginning in March 2009 and ending in October 2009. *Id.* at \*2.

During a deposition in December 2009, the defendant objected to the plaintiff’s use of two documents the defendant claimed were protected by the attorney-client privilege and had been inadvertently produced. *Id.* at \*2. Following the deposition, the defendant contacted the plaintiff to renew the objection and report that certain privileged documents meant to be withheld from the production had been inadvertently produced. *Id.* Four months later, the defendant provided the plaintiff with a document titled “Privilege Log-Documents Inadvertently Produced,” which identified 159

documents it claimed had been marked privileged during its review that should not have been included on the production website. *Id.* The defendant and the plaintiff resolved their dispute over all but six of the documents. *Id.* at \*2. The plaintiff then filed a motion seeking an order that the remaining six documents were either not protected by the attorney-client privilege or that the privilege had been waived. *Id.* at \*1. Magistrate Judge Schenkier granted this motion.

Under Federal Rule of Evidence 502(b), disclosure of privileged documents does not constitute a waiver of the privilege if: (1) the waiver was inadvertent; (2) the holder of the privilege took reasonable steps to prevent disclosure; and (3) the holder of the privilege took prompt steps to rectify the error. After examining the documents, Magistrate Judge Schenkier concluded that at least part of each document contained communications protected by the attorney-client privilege, *id.* at \*3-5, and he also found that the documents had been inadvertently produced. *Id.* at \*5-6. Magistrate Judge Schenkier then turned to the issue of whether the defendant took reasonable steps to prevent the disclosure. In considering that issue, he cited the Advisory Committee Notes to Fed. R. Evid. 502 and the “non-determinative guidelines,” which included “the reasonableness of the precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure, and the overriding issue of fairness.” *Id.* at \*6. Magistrate Judge found that “consideration of these factors leads the Court to find waiver.” *Id.*

First, he was unimpressed with the defendant’s submission to the Court describing what precautions it had taken to ensure privileged material was not produced. *Id.* at \*6. The defendant provided the court with only a broad overview of how it conducted the review, but did not provide a detailed account of its review procedure or submit an affidavit describing the steps taken by anyone who actually conducted the review. *Id.* The defendant stated that it “thought” the act of marking a document privileged meant that it would be withheld from the production database, but it appears the defendant never conducted a check to verify this point before the documents were published to the production website. Magistrate Judge Schenkier found the failure to conduct such a check to be “strong evidence of the inadequacy of the [defendant’s] precautions.” *Id.* at 7. In concluding that the defendant’s review procedures were inadequate, Magistrate Judge Schenkier observed:

“[E]ach and every document the [defendant] sought to retain as privileged was inadvertently disclosed to [the plaintiff]. It is ‘axiomatic that a screening procedure that fails to detect confidential documents that are actually listed as privileged is patently inadequate.’”

*Id.* at \*7 (citing *Harmony Gold U.S.A., Inc. v FAFSA Corp.*, 169 F.R.D. 113, 117 (N.D. Ill. 1996)).

Magistrate Judge Schenkier held that the defendant also failed to rectify the problem in a timely manner. While the defendant objected immediately to the use of the privileged documents when it learned of the problem in December 2009, and followed up with opposing counsel afterwards to renew its objection, by this point the defendant had been producing privileged documents on a rolling basis for over nine months and had not detected the error—a particularly notable oversight when “a single visit to the production database” would have detected the error. *Thorncreek*, 2011 WL 3489828, at \*8. The Magistrate Judge observed that had the defendant attempted to create a privilege log at an earlier date, the problem would have become known almost immediately. *Id.*

Having found the defendant failed to take reasonable precautions to prevent inadvertent disclosure of privileged documents, Magistrate Judge Schenkier held that privilege had been waived.

**4. In *Katiroll Co. v. Kati Roll and Platters, Inc.*, 2011 WL 3583408 (D.N.J. Aug. 3, 2011), Chief Judge Garrett E. Brown, Jr. ordered defendant restaurant, its owner, and his counsel to take various steps to address their failure to preserve certain electronic discovery, including ordering the defendant to briefly change his Facebook profile to include a prior photograph so that plaintiff could print Facebook pages as they existed prior to changes made by defendant.**

The underlying litigation was a trademark infringement suit involving two restaurants that sell a similar type of food, and the trade dress at issue involved the color of the restaurant, pictures of which were allegedly displayed on defendants' Facebook pages and website. *Id.* at \*1. Plaintiff moved the Court for spoliation sanctions and to compel discovery in connection with alleged discovery abuses, including disputes concerning the defendants' failure to preserve evidence contained on Facebook pages and the restaurant's website. *Id.* at \*2-3. The Court explained that, "[i]n determining whether spoliation sanctions are appropriate, the two key considerations are the 'degree of fault of the party who altered or destroyed the evidence' and 'the degree of prejudice suffered by the opposing party.'" *Id.* at \*1 (citations omitted). Plaintiff asked the Court to grant a "spoliation inference" for each of the alleged discovery abuses, which, as the Court explained, is the "mildest sanction" and "permits a jury to draw an adverse inference that the spoliated evidence might or would have been unfavorable to the position of the offending party." *Id.* at \*1 (citation omitted).

In connection with the disputes, the Court listed the four factors considered by New Jersey federal courts in resolving motions for a spoliation inference: (1) the evidence in question was within the party's control; (2) there has been actual suppression or withholding of the evidence; (3) the evidence destroyed or withheld was relevant to claims or defenses; and (4) it was reasonably foreseeable that the evidence would later be discoverable. *Id.* at \*1. There is a split in the District of New Jersey's jurisprudence as to whether the level of fault required to support the second factor is "intentional conduct" or mere negligence, and the Court concluded that "[w]here there is substantial prejudice to the opposing party, negligence may be sufficient to warrant a spoliation inference" and that "[w]here there is minimal prejudice to the opposing party, intentional conduct is required." *Id.* at \*2.

In considering the e-discovery abuses alleged by plaintiff, the Court first refused to sanction defendant for his failure to preserve his Facebook pages in their original state, reasoning that "Facebook took these pages down because of [plaintiff's] own take-down request." *Id.* at \*3. The Court explained that holding defendants responsible for this change to the Facebook pages would be unjust. *Id.*

Second, the Court considered plaintiff's request for a spoliation inference "based upon [defendants'] changing his profile picture on Facebook from a picture displaying the infringing trade dress without preserving that evidence." *Id.* at \*3-4. Regarding the first factor of whether the Facebook website was "in defendants' control," the Court held that this factor was present because it is more appropriate for defendants to have the burden given that "only defendants knew when the website would be changed." *Id.* at \*4. With regards to the second and fourth factors, the Court held that the spoliation was unintentional but nonetheless caused some prejudice to plaintiff. *Id.* In doing so, the Court explained that "the change of a profile picture on Facebook is a common occurrence" and that, therefore, "it is hardly surprising that [defendant] has changed his profile picture during the pendency of this litigation." Although both parties agreed that "changing the user's Facebook profile picture changes the picture associated with each and every post that user has made in the past," *id.* at \*3, the Court found that "it would not have been immediately clear [to defendant] that changing his profile picture would undermine discoverable evidence." *Id.* at \*4. Having considered these issues, the Court ordered defendants "to coordinate with plaintiff's counsel to change the picture back to the allegedly infringing picture for a brief time so that plaintiff may print whatever posts it thinks are relevant," adding that "such action shall not be considered an additional act of infringement." *Id.* at \*4.

Additionally, the Court concluded that defendants should have disclosed the existence of their new Facebook page in their discovery responses, but the Court held that sanctions were not appropriate given that plaintiff found the page

independently and that defendants created the page to comply with a preliminary injunction issued by the Court at the outset of the litigation. *Id.* at \*7.

Third, the Court ordered that, unless defendants promptly produced an image of their website showing what the restaurant had looked like prior to its repainting, the Court would grant a spoliation instruction on the limited issue of defendants' failure to produce such an image. *Id.* at \*5. The Court explained that "without the printout of the website, the evidence will be insufficient to show that the website itself embodied pictures of the infringing restaurant and substantial prejudice has accrued to plaintiff's ability to show that website itself infringed its trade dress." *Id.* Accordingly, the Court also ordered the defendant to search his home computer and to disclose any pictures of the restaurant prior to its repainting, noting that "it is implausible that [defendant] has no other electronic copies of these pictures on his hard drive or in emails to his web developer, etc." *Id.*

Fourth, with regards to defendants' production of a single email exchange in response to plaintiff's request for emails between defendant and his web developer, the Court found that a spoliation inference was not necessary to confirm whether other emails were sent. Instead, the Court directed defendants to take a series of steps to confirm whether such emails existed, noting that "[i]t seems suspicious that a person with as active an online persona as [defendant] only ever sent one email to his web developer . . ." *Id.* at \*6. The Court ordered (1) that defendant allow his counsel to search his email accounts and directed his counsel to produce any emails procured; (2) that defendants' counsel contact the web developer and request any emails exchanged with defendants; (3) that defendant was limited to contacting the web developer through counsel and only after receiving a response to the foregoing request for emails; and (4) that defendant request and produce phone records of any phone on which he made calls to the web developer. The Court denied plaintiff's request for a spoliation inference on this issue, reasoning that "the existence of such emails is too hypothetical to impose sanctions." *Id.* at \*6-7. Additionally, the Court directed defendants' counsel to "report every week to [the Court] by a brief letter submission on the progress of these investigations . . ." *Id.* at \*7.

Plaintiffs had also raised issues with regards to the timeliness and format of defendants' production of restaurant sales reports and other financial data. *Id.* at \*7. In contrast to its resolution of the novel e-discovery disputes described above, the Court stated that "these are run-of-the-mill discovery issues, on which the parties should confer to resolve." *Id.* Accordingly, the Court refused to sanction defendants or grant an order compelling production, reasoning that it did not believe either measure was "appropriate at this juncture." *Id.* Instead, the Court directed defendants' counsel to address the discovery issues in his weekly report until they are resolved. *Id.* Finally, the Court reminded both parties' counsel that they had an obligation to "confer in good faith prior to bringing issues before the Court" and to "creatively find solutions to common problems." *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](http://www.sidley.com/subscribe)

**[www.sidley.com](http://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.

