CHEAT SHEET

- In one case, a court issued sanctions for the deletion of a Facebook page during the course of litigation. In another, a judge said that once a plaintiff is "tagged" in photographs posted to social media sites, they are in the plaintiff's "possession, custody or control."
- Cloud computing, in which companies store data on third-party servers, is an emerging subject of law for the digital age; a few courts have held that even if data is not in the physical possession of its owner, it remains under that owner's control.
- Early rulings are divided as yet in cases of employees using their own electronic devices, such as cell phones, for work purposes. Historically courts have held that that an employer's control over its employees includes the right and ability to demand employment-related documents in their possession.

New Technologies Test the Limits of the Duty to Preserve, Collect and Produce Information in Civil Discovery

By Maggie Anthoney and J. Alexander Lawrence

Under the Federal Rules of Civil Procedure, it is fundamental that a party may seek documents that are in the opposing party's "possession, custody or control." The same or similar standards are reflected in most state civil procedure rules. The corollary to these rules is that to avoid claims of spoliation and the severe sanctions that may follow, a party is obligated to ensure such records are preserved when litigation is reasonably anticipated.

While the question of whether specific records are within a party's possession, custody or control has been heavily litigated for years, the digital revolution — with the advent of social media, cloud computing and mobile devices — has complicated the analysis. The answer to this important question has serious implications for almost all companies operating in the digital age.

The idea of control and who actually has it is still being clarified, but a fairly accepted definition looks at control as "the legal right, authority, or practical ability to obtain the materials sought on demand." *SEC v. Credit Bancorp, Ltd.,* 194 F.R.D. 469, 471 (S.D.N.Y. 2000). With that guidance, companies need to take a hard look at what material they may be found to have the right, authority, or practical ability to obtain, whether that is social media content, content stored in the cloud, or content from mobile or wearable devices.

Social media

The use of social media in recent years has exploded, with the proliferation of popular sites such as Facebook, Twitter, Instagram, Pinterest and LinkedIn. Likewise, to attract and retain a generation of workers accustomed to interacting online, companies have integrated social media tools like corporate wikis and chat tools into the work setting.

Whether those communication tools are internally or externally hosted, courts have made it clear that where relevant, the data generated through their use are discoverable. Likewise, courts have consistently found that data maintained on even externally hosted sites are within the company's control and must be preserved where litigation is reasonably anticipated and produced when relevant.

For instance, in a trade dress infringement case, *The Katiroll Co., Inc. v. Kati Roll and Platters, Inc.*, No 10-3620 US Dist. LEXIS 85212 (D.N.J. Aug. 3, 2011), the plaintiff moved for spoliation sanctions against the defendants after one of the defendants removed a Facebook profile picture, which showed the allegedly infringing trade dress, without preserving the appearance of the Facebook page prior to the change. The defendants argued that a finding of spoliation was unwarranted because the Facebook page was public and the plaintiff could have printed any relevant evidence at any time. The court disagreed, finding "public websites to be within the control of parties who own them" and calling the defendant's argument "an attempt to 'pass the buck' to Plaintiff to print websites that Defendants are obligated to produce." The court ordered the defendants to temporarily restore the picture depicting the alleged infringement so that the plaintiff could print any relevant content from the Facebook page.

Likewise, in *Gatto v. United Air Lines, Inc.*, No.: 10-cv-1090-ES-SCM, 2013 US Dist. LEXIS 41909 (D.N.J. March 25, 2013), the court issued sanctions for the deletion of a Facebook account during the course of litigation, finding "Plaintiffs' Facebook account was clearly within his control, as Plaintiff had authority to add, delete, or modify his account's content."

In *Davenport v. State Farm Mut. Auto. Ins. Co.*, No. 3:11-cv-632-J-JBT, 2012 US Dist. LEXIS 20944, at *2 (M.D. Fla. Feb. 21, 2012), the court held that the concept of control extends not only to photographs that a person may post to a social media site, like Facebook, but also to photos posted by others in which the individual is tagged. The court also held that once the plaintiff was tagged in the photos, they were in her "possession, custody, or control."

Similarly, in *Todd v. Tempur-Sealy Int'l, Inc.*, No. 13-cv-04984-JST, 2014 US Dist. LEXIS 161037, 4-5 (N.D. Cal. Nov. 16, 2014), the court held that with respect to social media pages regarding the defendants' mattresses, the company must produce "all responsive documents in their possession, custody or exclusive control, regardless of whether they are publicly available."

These cases demonstrate how companies have control over the social media content that employees create on behalf of the company or social media content that is stored on company owned equipment, as that content is information that a company has the legal right, authority or practical ability to obtain on demand. Because of this, companies must preserve and produce the data. Therefore, companies need to understand what social media content employees are creating and how to access those accounts in the event that the company comes under a duty to preserve and collect responsive information. Most of the larger social media platforms allow for easy collection of such data with user names and passwords, but knowing that it needs to be preserved is key.

Maggie Anthoney is corporate counsel at Lighthouse Discovery. Prior to joining Lighthouse, she worked for small and medium-sized law firms, as well as in-house at a start-up game company. Anthoney attended Whitman College where she studied politics and earned her JD from the University of Oregon School of Law. She is admitted to practice in Oregon and Washington State.
manthoney@lhediscovery.com

J. Alexander Lawrence is co-chair of Morrison & Foerster's E-Discovery Task Force and regularly advises clients on e-discovery issues and best practices. His practice involves all aspects of complex commercial litigation in federal and state trial and appellate courts, and in arbitration. He has represented US and international clients in actions involving IP rights, trade secrets, federal securities laws, the False Claims Act and a wide array of commercial disputes.
alawrence@mofo.com

Cloud computing

Once, businesses generally stored their business data on servers owned and operated by the company; it is now quite common for businesses to store critical information in the cloud. Again, while this data may no longer be in the business' "physical" possession or custody, it is certainly within the business's control.

Few courts have addressed this issue. Those that have generally find that businesses have a duty to provide relevant information stored in the cloud during the course of discovery and to preserve such data where litigation is reasonably anticipated. For instance, in *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093 FMC(JCx), 2007 US Dist. LEXIS 46364, 25-26 (C.D. Cal. May 29, 2007), the defendant took the position that certain server log data was not within its possession, custody, or control because it was routed through a third party, Panther, with whom the defendant contracted. The court held that "even though the Server Log Data is now routed to Panther and is temporarily stored in Panther's RAM, the data remains in defendants' possession, custody or control."

Other courts have reached the same conclusion: Information stored in the cloud may be discoverable and should be preserved where it is within a party's control. See, *e.g., SEC v. Estate of Saviano,* 2:14-cv-13902-MOB-MKM, 2014 US Dist. LEXIS 143714 (E.D. Mich. Oct. 9, 2014) (holding an order prohibiting the destruction of records "extends to the preservation and retention of Evidence in the possession or custody of third-parties, such as an internet service provider or a cloud computing provider, if such Evidence is within Defendants' control."); and *e-Merging Mkt. Techs., LLC v. Elk Auto. Components Shanghai Gaoqi Auto. Components*, No. 08-15150, 2013 US Dist. LEXIS 23661 (E.D. Mich. Feb. 21, 2013) ("SL America must produce to Plaintiff all documents identified in the subpoena at issue in this motion that are within SL America's possession, custody, or control, including but not limited to any responsive documents of SL Tennessee which SL America has control of through their shared ERP or cloud storage system.")

Similar to the analysis with respect to social media content, companies must be aware of the data that are stored in the cloud and the control that they exercise over the data. If the company has the legal right, authority or practical ability to obtain documents or other data from the cloud, it's likely that a court will determine that the company has control over that data and so must preserve and produce the information if it is deemed relevant.

Mobile and wearable devices

From smartphones to wearable devices, the use of personal electronic devices by employees is on the rise. As a result, employees increasingly use such devices both at work and at home, for both work and personal purposes. This expanded use companies allowing of personal electronic devices in the workplace, so called "Bring Your Own Device" policies, raises difficult issues in litigation.

Again, the general rule is that a party served with document requests is required to produce responsive documents within its "possession, custody, or control." If the party does not actually have the document in hand, courts look to see whether the party has control of it — as noted above, construing the word "control" broadly as the right, authority or practical ability to obtain the document upon demand of the party who does possess it. Reasoning that an employer's control over its employees includes the right and ability to demand employment-related documents in their possession, courts have consistently held that employers have a duty to collect and produce responsive documents held by their employees. However, determining the line between

Determining the line between what are employer documents on an employee's personal electronic device and what are an employee's private data is still a gray area.

Companies should look hard at their policies around employee use of social media, cloud computing and mobile devices. If companies have polices around their use, they can take a more proactive role in clearly defining what they have control over.

what are employer documents on an employee's personal electronic device and what are an employee's private data is still a gray area that courts must answer in order to determine whether a company has complied with its duty to preserve and produce responsive documents.

In *Cotton v. Costco Wholesale Corp.*, No. 12-2731-JWL, 2013 US Dist. Lexis 103369 (D. Kan. July 24, 2013), however, the court did not compel the employer to produce employee emails and texts. In that case, the plaintiff sought text messages sent or received by two Costco employees from their cell phones relevant to the plaintiff's claims. The court noted that the plaintiff did not "contend that Costco issued the cell phones to these employees, that the employees used the cell phones for any work-related purpose, or that Costco otherwise has any legal right to obtain employee text messages on demand." Thus, the court held that "Costco does not likely have within its possession, custody, or control text messages sent or received by these individuals on their personal cell phones." Of the factors cited by the court, it would seem that the complete lack of any showing that the employees used their personal devices for work purposes is the most critical.

Another court found that business-related text messages on employees' personal cell phones were subject to preservation and production requests in *In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation,* MDL No. 2385, 2013 US Dist. Lewis 173674 (S.D. Ill. Dec. 9, 2013). The defendants raised the issue that some employees use their personal cell phones while on business and use the texting feature of those phones for business purposes yet balked at the request of litigation lawyers to examine personal phones. The court held that the litigation hold and the requirement to produce relevant text messages, without question, applies to that space on employees' cell phones dedicated to the business that is being litigated, and that any employee who refused to turn off the auto delete feature for text messages or refused to turn over his or her phone for the court's examination of the relevant space on the phone would be subject to a show cause order. The employee would then need to appear personally to demonstrate why he or she should not be held in contempt of court.

To the extent that employees use personal devices for work purposes, the question is raised of how far an employer must go to collect relevant documents from its employees' personal devices. Does it suffice for the employer to request that the employee search his own devices for responsive documents, or must the employer collect the devices and search them in the same manner that it searches company-owned devices? The answer is unclear, but will likely depend on whether a court is comfortable that all relevant information is being collected and produced through less intrusive means.

While being aware of these issues are important for companies, companies should look hard at their policies around employee use of social media, cloud computing and mobile devices. If companies have polices around their use, they can take a more proactive role in clearly defining what they have control over rather than waiting for a court to determine after the fact whether they had control or not. In examining such policies companies should make sure to pay attention to their own company culture, the cross-company impact of such policies, what the appropriate platforms for their business use are, and training employees on what is expected of them with respect to their use. Some strategic thinking by companies prior to a preservation request will help to ensure that companies preserve and produce appropriate material on the front end rather than being subject to sanctions for potential spoliation of evidence for not preserving such information. **ACC**

ACC EXTRAS ON… Discovery trends

Top Ten
Top Ten Ediscovery US Trends in 2015 (Mar. 2015).
www.acc.com/topten/ed_mar15

Program Materials
The New Frontier: Data and Discovery in a New Era of Technology (Oct. 2014).
www.acc.com/pm/data_oct14

New Federal Rules Changes and the Cost of Discovery (Oct. 2014).
www.acc.com/pm/discovery-cost_oct14

QuickCounsel
Cloud Computing in Ediscovery and Information Governance (Jan. 2012).
www.acc.com/quickcoun/cloud&ig_jan12

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

McDermott
Will & Emery

The Art of Client Service.

At McDermott Will & Emery, superior client service and cohesive collaboration are paramount to our business culture and values. We harness our local market knowledge and geographic reach to deliver innovative solutions to our clients and communities.

www.mwe.com