Social Media and Antitrust: A Discovery Primer

BY NATHANIEL C. GIDDINGS AND AARON PATTON

As our economy has shifted to the online marketplace, so too have the communications that can give rise to antitrust liability. Recent cases suggest that at least some communications evincing unlawful antitrust violations have migrated to social networking sites (SNS), such as Facebook and Snapchat. Indeed, the DOJ recently obtained a guilty plea and a $1.9 million criminal fine from “[a]n e-commerce company and its top executive” for conspiring through SNS and encrypted messaging applications, including Facebook, Skype, and WhatsApp. While these communications are generally discoverable, preserving and producing (or acquiring) material from SNS can be a difficult and time-consuming process in which there are certain pitfalls (and costs) that attorneys should be mindful of when addressing this type of discovery.

Obtaining Social Media Evidence

First Order Pitfalls: Thinking About Ethical Rules and Federal and State Law. Material on SNS that may be reasonably calculated to lead to admissible evidence include private bilateral or direct message communications (e.g., Facebook or Twitter “DMs”), private group communications (e.g., a “closed,” “private,” or “secret” Facebook group), or a private profile (e.g., a Facebook profile that restricts access to some or all content on the profile). While it would certainly be easiest to attempt to acquire this non-public material by “friending” the individual or through a “friend” of the sought-after individual, counsel must consider the applicable rules of professional conduct before undertaking such an action. This is true regardless of whether the individual is employed by a company that has a policy that purports to “own” its employees’ social media content or whether the lawyer directly attempts to access this material or hires another individual to do it by proxy. While a case-by-case analysis would be necessary, proceeding through formal discovery channels should help avoid any ethical concerns when seeking these communications.

State Privacy Laws May Apply. Attorneys must also consider any applicable state privacy laws that may limit their ability to collect SNS material. According to the Sedona Conference, “Many states have enacted legislation that specifically prohibit an employer from seeking such information from an employee, and an employer’s attempt to solicit an employee’s usernames and passwords to facilitate a social media capture may violate those states’ privacy statutes.” As with the ethical rules, proceeding through the formal discovery process may alleviate these concerns.

Federal Law Limits the Types of Material a Private Litigant Can Acquire Directly from Providers of SNS. The Stored Communications Act (SCA) governs the sharing of “stored wire and electronic communications and transactional records” in the possession of “Internet service providers.” Courts have generally concluded that providers of SNS are “Internet service providers” under the SCA, and, as a result, private litigants are unlikely to be able to acquire electronic communications (e.g., posts on a private Facebook wall) from the provider itself. For instance, in Crispin v. Christian Audigier, the U.S. District Court for the District of New Jersey, citing to the SCA, quashed a subpoena directed to Facebook that sought the contents of private communications occurring on that site.

However, courts have held that private litigants can acquire “transactional” records from the providers of SNS. Transactional information includes, for instance, “record information regarding the characteristics of the message that is generated in the course of the communication” and “identifying information associated with the subscriber as well as the usage information of each account for certain time periods.” This information may be useful to a private litigant attempting to understand the scope (i.e., burden) of preserving, acquiring, or producing this material before undertaking the steps necessary to do so.

My Case Involves Potentially Relevant Material on SNS—What Should I Do? Preserve the Potentially Relevant SNS Material. Although private litigants are unlikely to acquire electronic communications directly from providers of SNS, courts have held that the contents of the communications occurring on (and stored by) the provider can be acquired through party or non-party discovery directed to individuals and entities other than the provider. This being the case, “as soon as a party is on notice of actual or reasonably anticipated litigation, counsel should implement a litigation hold that accounts for potentially relevant social media evidence that is in the possession, custody or control of his or her client.” This litigation hold...
should include the contents of any communications, any backups, and the associated metadata for both.\textsuperscript{17}

An employer should also take steps to preserve its employees’ social media accounts material (e.g., through a litigation hold) and ask its current and former employees whether they are willing to provide access to their personal social media accounts.\textsuperscript{18} While no court has held that a company has “control” over its employees’ social media accounts,\textsuperscript{19} at least one court has compelled a company to search for and produce documents from its employees’ personal email accounts.\textsuperscript{20} Similar rationales could be applied to employees’ personal social media accounts, and, as such, whether a court would hold that a company has “control” over its employees’ social media postings will likely depend on the specific facts of the case.\textsuperscript{21}

Serve a Discovery Request for this Material on the Parties. As with any other discovery, a private litigant must first attempt to obtain material on SNS from parties to the litigation.\textsuperscript{22} While this does not mean that the party necessarily needs to “exhaust” party discovery by, for instance, moving to compel the party for the discovery, before pursuing third party discovery,\textsuperscript{23} a private litigant should take reasonable steps to acquire this information from an opposing party in the first instance.

Respond to the Discovery Request. A private litigant has several decisions to make when confronted with a discovery request seeking “all” of its (or its employees’) communications occurring on SNS.

First, courts addressing the discoverability of social media evidence from a party opponent generally conclude that this SNS material is in the party’s “control” (and therefore discoverable) when it is the party’s own content.\textsuperscript{24} For example, in Heyman \textit{v.} Nevada, the U.S. District Court for Nevada “instructed Defendant’s counsel to review Defendant’s social media content and produce any relevant, nonprivileged content contained therein.”\textsuperscript{25} The same would be true for a social media site managed by the party. In \textit{Arteria Property PTY Ltd. v. Universal Funding V.T.O., Inc.}, for instance, the U.S. District Court for New Jersey imposed sanctions on a company that destroyed its website “as it existed during the time that the dispute between the parties first arose” because the defendant had “the ultimate authority, and thus control, to add, delete, or modify the website’s content.”\textsuperscript{26} The foregoing is true regardless of whether the party has itself stored the material.\textsuperscript{27}

Second, regardless of whether a party ultimately decides to produce material on SNS, it should disclose the existence of this material,\textsuperscript{28} and if the party responding to the request is taking the position that this material is beyond its possession, custody, or control, it should explicitly state as much in its responses and objections.\textsuperscript{29}

Serve a Subpoena for this Material on a Third Party. If a litigant is unable to secure the production of this material from the opposing party, it should consider whether the information may be obtained through a subpoena to a third party. While it is not possible to get the electronic communications directly from the provider of the SNS, courts have routinely held that the SCA’s protections do not extend to individuals using an SNS or administering a “group” using the site’s facilities.\textsuperscript{30} In \textit{Nucci v. Target Corp.}, the plaintiff petitioned the Florida District Court of Appeals “for certiorari relief to quash a December 12, 2013 order compelling discovery of photographs from her Facebook account.”\textsuperscript{31} In support of her petition, the plaintiff argued, in part, that the SCA shielded her Facebook account from discovery. The court rejected this argument and denied the petition:

\begin{quote}
[W]e reject the claim that the Stored Communications Act has any application to this case. Generally, the “SCA prevents ‘providers’ of communication services from divulging private communications to certain entities and/or individuals.” The act does not apply to individuals who use the communications services provided.\textsuperscript{32}
\end{quote}

Courts have also generally rejected arguments from third parties that discovery of communications occurring on SNS would violate their privacy rights.\textsuperscript{33} This is especially true where there is a protective order in place that limits the use of the allegedly “private” information.\textsuperscript{34}

Finally, a third party can always assert a burden objection. One potential way to overcome this objection—and ensure that this material is collected in a way that minimizes the risk that it is later excluded (as discussed below)—is to offer to pay for the professional collection of the material.\textsuperscript{35}

\textbf{How to Collect \& Review Material from SNS.} Once it has been determined that SNS material \textit{will} be produced, the next question is how it should be collected for production.

Because courts have been reluctant to admit mere screenshots of webpages or social media sites under Federal Rule of Evidence 901,\textsuperscript{36} it is advisable to engage a certified forensic examiner to collect the material on SNS so that all relevant metadata—including information identifying the parties to the communications—is maintained and the forensic examiner can submit a declaration regarding the collection methodology. For example, in \textit{Commonwealth v. Banas}, the Appeals Court of Massachusetts found that the trial court properly excluded a printout of a picture from Facebook because “evidence that a message was from an individual’s Web page was not sufficient to authenticate that the individual wrote the message.”\textsuperscript{37} Engaging a certified forensic examiner to collect the material in question can help avoid this pitfall when this material is sought to be introduced.

Because providers of SNS do not generally include litigation discovery tools as part of their platforms (at least not yet), preserving and collecting material on SNS also requires special purpose software.\textsuperscript{38} Software tools, like X1 Social Discovery, are preservation and collection applications created, developed, and maintained by outside companies that work within the rules and policies of each SNS’s Application Programming Interface (API) and Software Developer Kit (SDK).\textsuperscript{39} Therefore, what can be collected will generally be
what is publicly available and what can be accessed given the user’s account permissions.

When using a software tool to collect this material, counsel can either conduct a “Credentialed User,” an “Examiner,” or a “Web Crawl” collection. A “Credentialed User” collection is used to collect non-public information using account credentials of a user with permission to access the data. Similarly, to collect non-public data from a private group (e.g., posts and membership rosters), a forensic examiner would either need a group member’s credentials or its own account added to a group’s membership by another member or administrator of the group.

An “Examiner” collection is used to collect public information (e.g., public tweets, posts, comments, images, etc.). This collection method works by having the forensic examiner create a “shell” or “examiner account” and then create a targeted index of a user’s or group’s publicly available data.

Finally, a Web Crawl collection works by “crawling” through a website’s URL, deeper and deeper, capturing web content while taking snapshots of the pages with their web-enabled content fully rendered and collecting and hashing all of the web elements for authentication.

**Limitations to Collection of Material from SNS.**

While these specialized software tools are the best means of collecting this material, they can also be limited in three important ways: by the SNS, by the software itself, and by the user.

SNS providers, such as Facebook and Twitter, have unfathomable and continually growing amounts of data to store and present. This means it is impractical (and likely impossible) for platforms to present all of their user data for public use or even allow access to it all through their User Interface.

Attorneys should, therefore, consider and agree with opposing counsel on any limitations on the number of layers that can be collected from SNS. For instance, X1 Social Discovery allows examiners to set the number of layers it indexes and collects, with a limit of ten layers. While ten layers is usually sufficient for Credentialed account collections, in large groups or the accounts of particularly active users (e.g., celebrities), there can be substantially more than ten layers. Since the tools cannot expand layers beyond the tenth for indexing, the collected data will contain indications of uncollected data.

There is also the possibility that material on SNS has been altered, edited, or deleted. While counsel facing a potential destruction issue could attempt to determine the scope of the problem through testimony or screenshots, counsel could also undertake a “rescan” with the social media collection software. The rescan works the same as the initial collection. However, this option requires an initial collection, before any changes or deletions, as the baseline against which to compare. If data is deleted or altered before an initial scan, even when there are references to deleted content, evidentiary options could be limited.

Consider the Costs and Benefits of Each Collection Method. There is a trade-off between an Examiner or Credentialed User collection on the one hand and a Web Crawl collection on the other. The former collection methods capture more metadata than the Web Crawl method, and they are usually faster than a Web Crawl. Whereas a Credentialed Facebook collection’s metadata would contain up to 75 fields (including Captions, Number of Comments, Likes, and Geo Location), a Web Crawl collects up to 23 metadata fields—
not including the previous field examples. The difference in the total number and actual fields captured is a function of collecting actual posts from SNS versus posts that are collected as webpages. It is also worth noting that Web Crawls usually result in larger collections, and they are usually slower to finish because they "crawl" through a link’s layers, opening and rendering web pages and layers for capture and hashing. The advantage of a Web Crawl is that it accesses and collects more "layers" of information than an Examiner or Credentialed User collection.

Counsel should consider these differences before deciding on a collection method. However, it may not be immediately apparent which option is necessary, meaning that the collecting party may need to attempt different collection iterations to find the "best available" option.

Consider Options for Export and Review. Reviewing and using material collected from SNS is like all things in today’s discovery: imperfect. While tools like X1 Social Discovery can export common review platform load files (.DAT), natives (MHTML, HTML), images (PNG), and text (embedded in .DAT), working with the export is another trade-off. For example, while tools like Relativity have a viewer that can render MHTML and HTML files collected from Facebook or Twitter, if the Relativity platform is locked away from accessing the web, then the web-enabled content (OLEs, etc.) that references Internet locations will not load or render. The result in the review platform viewer is a broken-looking webpage that is not ideal for use as evidence or for review. The alternative is to review the PNG image files, but these are not ideal either. The PNG will be a single-image screen capture of a page with all of its web content enabled. That sounds ideal because the PNG will look just like a post would appear in the UI, but if the post has many comments or replies, the resulting PNG image will shrink the web page to fit all the content into a single image. The result for larger posts or threads is a very large image file with very small content that can only be viewed by using the zoom feature in the viewer.

Conclusion

Social media is here to stay, and it can be among the most revealing evidence in a case. Attorneys should be prepared to answer questions about their clients’ preservation, collection, and production of material from SNS when and if litigation occurs and should closely monitor this ever evolving area of discovery practice.

---

1 See Jeffrey S. Tennenbaum & A.J. Zottola, The Legal Aspects of Online Social Networks: an Overview for Associations, N.Y. Soc’y of Ass’n Executives (Dec. 2009), https://www.nysaenet.org/resources1/inviewnewsletter/pastissues/2009/december2009/inview122009_article4 (“Social networking sites and related media can make it easy for members to let their guard down and share information that could lead to a violation of the antitrust laws. An association should, therefore, ensure that it applies and enforces its existing antitrust policies with respect to social networking sites.”).


4 See generally Johnson v. PPI Tech. Servs., L.P., No. 11-2773, 2013 WL 4508128, at *1 (E.D. La. Aug. 22, 2013) (“Courts have recognized that social networking site (‘SNS’) content may be subject to discovery under Federal Rule of Civil Procedure 34.”) (citations omitted); see also Forman v. Henkin, 30 N.Y.3d 656 (N.Y. 2018).


6 See MODEL RULES OF PROF’L CONDUCT 4.2; 4.4; see also N.Y. City Bar Formal Opinion 2010-2.

7 See Steven C. Bennett, Civil Discovery of Social Networking Information, 39 SW. L. REV. 413, 418–19 (2010) (“[M]any companies expressly inform their employees that any and all documents and information created, stored or exchanged from or by the employer’s computer and communications systems belong to the employer. As a result (arguably), such companies could be held to ‘control’ all such information, even if created for personal use, and even if physically stored on a third party’s servers.”) (footnotes omitted).

8 See MODEL RULES OF PROF’L CONDUCT 8.4(a) (It is professional misconduct to “knowingly assist or induce another,” or “through the acts of another,” to violate the Rules of Professional Conduct.).

9 The Sedona Conference Commentary on Rule 34 and Rule 45 “Possession, Custody, or Control,” 17 SEDONA CONF. J. 467, 524–25 (2016).


11 See generally Levine v. Culligan of Fla., Inc., No. 50-2011-CA-010339, 2013 WL 1100404, at *3 (Fla. Cir. Ct. Jan. 29, 2013) ([C]ourts seem to be in agreement that the [SCA] prohibits records from being subpoenaed directly from Facebook and other social networking sites.”) (citing cases).


13 In re Zynga Privacy Litig., 750 F.3d 1098, 1104–06 (9th Cir. 2014).


17 Sara Anne Hoek & Cori Faklaris, Oh, Snap! The State of Electronic Discovery Amid the Rise of Snapchat, Whatsapp, Kik, and Other Mobile Messaging Apps, FED. L. W. May 2016, at 64, 70.


19 The Sedona Conference Commentary, supra note 9, at 524 (“While some have attempted to argue that under the Practical Ability Standard, corpora-
tions may have the ‘practical ability’ to obtain data from social media sites they do not own or control merely by asking their employees to preserve/produce it, no court has specifically held this to be true.”


21 For example, a company policy that states that an employee’s activity on the company’s network belongs to the employer may lead a court to conclude that the company has “control” over its employees’ SNS material. See Bennett, supra note 7, at 419.


24 See generally The Sedona Conference® Primer on Social Media, 14 Sedona Conf. J. 191, 224 (2013) (“A user typically has ‘control’ of his or her own social media content—to the extent he or she can still access it—because the user typically has the ‘legal right, authority, or practical ability to obtain the materials sought on demand.’”).


28 How Can I Download My Information from Facebook?, FACEBOOK, https://www.facebook.com/help/212802592074644 (Steps to Download My Data); see also General Account Settings, FACEBOOK, https://www.facebook.com/dy undx=AdloyGBwq2PsPixo (Link to Download My Data); Accessing Your Facebook Data, FACEBOOK, https://www.facebook.com/help/405183566 (Steps to Download My Data). For example, while Facebook offers an option for individuals to “download” their own data, and the data points included are robust, the platform does not allow users to download others’ data nor is the resulting archived format used for litigation.

29 Application Programming Interface, WIKIPEDIA, https://en.wikipedia.org/wiki/Application_programming_interface (“An application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software [...] A good API makes it easier to develop a computer program by providing all the building blocks, which are then put together by the programmer.”); Software Development Kit, WIKIPEDIA, https://en.wikipedia.org/wiki/Software_development_kit (“A software development kit (SDK or devkit) is typically a set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform. To enrich applications with advanced functionalities, advertisements, push notifications and more, most app developers implement specific software development kits.”). In fact, X1 Social Discovery states in their product description, and in bold font, that “X1 Social Discovery cannot be used to bypass or violate the privacy or security settings of any social network.” Product Description, X1 SOCIAL DISCOVERY, http://help.x1sd.com/productdescription.

30 Main Features of X1 Social Discovery, X1 SOCIAL DISCOVERY, http://help.x1sd.com/features (providing definitions for Credentialed User and Examiner collections).

31 It is worth noting that X1 Social Discovery does not collect data from “private” or “secret” Facebook profiles or groups unless proper authorization is provided. This limitation is intentional and is in line with its policy to not “bypass or violate the privacy or security settings of any social network.” Product Description, X1 SOCIAL DISCOVERY, http://help.x1sd.com/product_description.

32 Id.


and production of ESI. Moreover, where counsel are using keyword searches for retrieval of ESI, they at a minimum must carefully craft the appropriate keywords, with input from the ESI’s custodians as to the words and abbreviations they use, and the proposed methodology must be quality control tested to assure accuracy in retrieval and elimination of ‘false positives.’ It is time that the Bar—even those lawyers who did not come of age in the computer era—understand this.”).

45 Create a Web Capture or Crawling Collection, X1 Social Discovery, http://help.x1sd.com/create-a-web-crawl-collection (“A layer consists of all the links directly related to that page.”).

46 Id. (“You can set a limit as to how many Layers down, from the top-level domain, X1 Social Discovery will crawl and index by selecting the Layers checkbox and entering a value. The maximum number of Layers is currently capped at 10 and defaulted to 5.”)


49 See Facebook Metadata Fields, X1 Social Discovery, http://help.x1sd.com/facebook-metadata-fields (Full list of metadata fields).

50 See Web Capture Metadata Fields, X1 Social Discovery, http://help.x1sd.com/web-capture-metadata-fields (Web capture has up to 23 metadata fields).

51 The collection of 10 layers for a large group could result in over 100 gigabytes of SNS material, and it could take over two weeks to collect.

52 Main Features of X1 Social Discovery, X1 Social Discovery, http://help.x1sd.com/features (“A Credentialed Facebook Account has the ability to index a user’s Posts, User Information, Private Messages—Limit of 5000 per Conversation, Photos, Posts from selected Friends and Friends of Friends (depending on FB Privacy Settings) and ability for users to view (on a map) the location where posts are made where Geo Location information is available.”).