Bloomberg BNA

Social Media Law & Policy Report™

PRIVACY

Two recent federal district court rulings have held that the Stored Communications Act protects the private online pages of Facebook users. The author summarizes those two rulings and the contours of the SCA, and he offers a critique of the rulings. He concludes that restricting the ability of civil litigants to access private social media content would be potentially the most significant outcome of the two cases, were their reasoning adopted by others courts.

Social Media and the Stored Communications Act: Does a 1986 Law Protect Timelines and Tweets?

BY TODD C. TAYLOR

On Aug. 20, 2013, Judge William J. Martini, a New Jersey federal district court judge, granted a summary judgment motion in favor of an employer in the case of *Ehling v. Monmouth-Ocean Hospital Service Corp.*[1]

At first glance, the case appeared to be nothing more than a fairly routine dispute between the Monmouth-Ocean Hospital Service Corp. (MONOC) and Deborah Ehling, a former MONOC employee. However, *Ehling*, at least in part, involved Facebook and online privacy rights. Specifically, in the course of his ruling, Martini found that the Stored Communications Act (SCA)[2] protects private online pages of Facebook users.

Two questions arise from *Ehling* (and another recent SCA case that will be discussed below):

- Are courts correct in deciding that the SCA applies to social media sites?
- What are the practical implications of these recent court rulings applying the SCA to social media?

The Facts of Ehling

From 2004 until the termination of her employment in 2012, Ehling worked as a nurse-paramedic for MONOC, a nonprofit hospital providing emergency medical services in New Jersey. On June 8, 2009, while still employed by MONOC, Ehling posted the following to the wall[3] of her Facebook account:

> An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children).

[1] *Ehling v. Monmouth-Ocean Hospital Service Corp.*, No. 2:11-cv-03305, 2013 BL 220816 (D.N.J. Aug. 20, 2013).

Todd C. Taylor is a Senior Counsel in the Commercial & Technology Transactions and the Privacy & Data Security practice groups at Moore & Van Allen PLLC.

[2] 18 U.S.C. §§ 2701 – 2712.

[3] The Facebook wall has since been replaced by the Facebook timeline. See Jill Duffy, *12 Things You Should Know About Facebook Timeline*, PC Magazine, Jan. 25, 2012, *available at* http://www.pcmag.com/article2/0,2817,2393464,00.asp.

> Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other guards. . . .go to target practice.[4]

Based on her Facebook privacy settings, only Ehling's 300 or so Facebook friends could view the post. Tim Ronco was one of those friends. Ronco, for reasons known only to him, decided to share Ehling's post with MONOC management. Once it was aware of Ehling's post, MONOC management temporarily suspended Ehling on the basis that her comment reflected a ''deliberate disregard for patient safety.''[5]

Over the ensuing years, until her ultimate termination of employment in 2012, Ehling had a rocky relationship with MONOC. In 2011, while still employed by MONOC, she filed suit against them. Her complaint included an allegation that MONOC violated her rights under the SCA by improperly accessing her Facebook wall post.[6]

The SCA

Before analyzing *Ehling* any further, a quick tour of the SCA is warranted.

The SCA, part of the broader Electronic Communications Privacy Act (ECPA), was signed into law by President Ronald Reagan on Oct. 21, 1986.[7] At the time of the law's passage, Mark Zuckerberg (Facebook's founder) was 2 years old.

The SCA was intended to provide computer network account holders some basic statutory privacy protections for their electronic communications and records in the possession of third-party providers.[8] The SCA, among other things, includes the following key provisions:

- Section 2701(a) of the SCA criminalizes intentional, unauthorized access to stored electronic communications held by an electronic communications service (ECS).
- Section 2702 of the SCA prohibits ECS providers and remote computing services (RCS) providers from disclosing user communications (subject to certain express conditions and exceptions).
- Section 2703 of the SCA sets forth the process by which the ***government*** can (a) obtain electronic communications and other records from ECS and RCS providers and (b) require such providers to maintain backup copies of identified communications.

To better comprehend the SCA, the following key terms, used throughout the SCA, should be understood:

- *Electronic Communication*—basically a transfer of data (such as text, images or sound) by wire, radio or electronic systems.[9]
- *Electronic Communication Service, or ECS*—a service providing users the ability to send or receive electronic communications.[10]
- *Electronic Storage*—
  - o ''any temporary, intermediate storage'' of electronic communications in connection with their transmission; and
  - o any storage of electronic communications by an ECS provider ''for purposes of backup protection[.]''[11]

The Ehling SCA Ruling

In *Ehling*, Martini was faced with the question of whether MONOC violated Section 2701(a) of the SCA when it received Ehling's private Facebook wall posts. In order to analyze this issue, Martini had to first determine whether the SCA applied to non-public Facebook wall posts. He concluded that it did.

In reaching this conclusion, the court noted that Facebook wall posts are electronic communications within the meaning of the SCA, as such posts involve the transmission of text or images from a user's computing device to Facebook's servers via the Internet.[12] The court's conclusion on this point is clearly supported by the SCA.

Next, Martini found that Facebook wall posts are transmitted via an ''electronic communication service.''[13] It is difficult to dispute this conclusion. The core feature of the Facebook service is to allow users to communicate with others via public and private posts transmitted electronically over the Internet.

The court then ruled that Facebook wall posts are in electronic storage. As we saw above, an electronic communication can meet the electronic storage test if (a) it is in temporary, intermediate storage in connection with its electronic transmission (e.g., e-mails that are temporarily stored on the servers of e-mail or Internet service providers prior to being opened and locally downloaded by an end user) or (b) it is stored by the ECS provider for purposes of backup protection. The court quickly found that Facebook ''wall posts are not held somewhere temporarily before they are delivered,'' and consequently they would not meet the temporary, intermediate storage test.[14] The court nonetheless found that Facebook wall posts were stored for backup purposes ''[b]ecause Facebook saves and archives wall posts indefinitely.''[15]

Having found that the elements of a violation of Section 2701(a) of the SCA had, to that point, all been met, the court felt compelled to point out that Facebook walls posts that are configured to be private are deserving of the SCA's protection.[16] It is not entirely clear why the court mentioned this point, as Section 2701(a) does

---

[4] *Ehling*, 2013 BL 220816, at *2-*3.
[5] *Id*. at *3.
[6] *Id*. at *1- *4.
[7] Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986). *See also* David Kravets, *Aging 'Privacy' Law Leaves Cloud E-Mail Open to Cops*, WIRED (Oct. 21, 2011, 6:30 AM), http://www.wired.com/threatlevel/2011/10/ecpa-turns-twenty-five (providing background and context relating to passage of ECPA).
[8] See 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, 1209-14 (2004).
[9] 18 U.S.C. § 2510(12).
[10] 18 U.S.C. § 2510(17).
[11] 18 U.S.C. § 2510(17).
[12] *Ehling*, 2013 BL 220816, at *7.
[13] *Id*.
[14] *Id*.
[15] *Id* at *8.
[16] *See id*.

  ISSN

not expressly make a distinction between public and private electronic communications—though admittedly other parts of the ECPA exempt publicly available communications from the SCA's coverage.[17]

Still, the court did not find in Ehling's favor on the SCA issue. Since Ronco, one of Ehling's Facebook friends with access rights to her private wall, had properly accessed the communication and voluntarily provided it to MONOC management on an unsolicited basis, Martini ruled that MONOC was not in violation of Section 2701(a).[18] That conclusion was based on language in Section 2701(c) of the SCA that specifically exempts from Section 2701(a) coverage any ''conduct authorized . . . by a user of [an electronic communication service, such as Facebook] with respect to a communication of or intended for that user[.]''

The Crispin Case

At least one other court has also concluded that the SCA applies to social media sites. In 2010, the U.S. District Court for the Central District of California, in the case of *Crispin v. Christian Audigier, Inc.*, found that both Myspace and Facebook were ECS providers covered by the SCA.[19]

Crispin presented somewhat different facts than *Ehling*. Buckley Crispin was an artist who had granted an oral license to his artwork to Christian Audigier Inc. Crispin brought suit against Audigier, claiming that Audigier had granted sublicenses outside of the scope of the license granted by Crispin.[20]

In connection with the dispute, Audigier served subpoenas on several social networking websites (including Facebook and Myspace). The subpoenas sought certain communications that Crispin had made on the sites. Crispin moved to quash the subpoenas on a number of different grounds, including that the social media sites were prohibited from disclosing his communications pursuant to the SCA.

In the course of its opinion, the *Crispin* court reached the following conclusions:

- Myspace and Facebook were both ECS providers.[21]
- Myspace comments and Facebook wall postings, once made, are electronic communications that are stored for backup purposes and therefore are in electronic storage within the meaning of the SCA.[22]
- An ECS provider generally is not permitted to release electronic communications in electronic storage pursuant to a subpoena duces tecum issued in civil litigation involving private parties. As a general rule, the statute only permits such information to be released pursuant to a governmental entity in accordance with certain provisions of the SCA.[23]

Based on those conclusions, the court quashed Audigier's subpoenas that sought private messages posted on the social media sites.[24]

Were Ehling and Crispin Rightly Decided—Should the SCA Apply to Private Spaces on Social Media Sites?

Were the Private Posts in Ehling and Crispin in Electronic Storage?

It is highly debatable whether *Ehling* and *Crispin* were correctly decided (at least on the issue of whether private social media pages are in electronic storage). Both cases based much of their SCA rulings on the fact that the electronic communications at issue were intended to be private. Although it is true that the SCA does ***not*** protect information that is publicly available,[25] that does not mean that the SCA protects all private electronic communications. Sections 2701 and 2702 of the SCA prohibit unauthorized access and disclosure of electronic communications held by electronic communications providers if those communications are in ''electronic storage.'' If an electronic communication is private—but not in electronic storage—it would not be protected under either Section 2701(a) or 2702(a)(1) of the SCA.

Both *Ehling* and *Crispin* concluded that privacy-protected posts on social media sites were in electronic storage, as they were created for purposes of backup protection. But this conclusion seems forced at best, and it ignores how social media sites operate. A user who chooses privacy protection on a site such as Facebook is generally not doing so to protect the information for purposes of future retrieval and access. Instead, the person is typically posting the protected content for the purposes of being viewed, if only by a more limited number of users (though given that Ehling had 300 Facebook friends—it is doubtful that she thought much about the privacy of her Facebook posts at all).

There is a reason Facebook, Twitter, LinkedIn, MySpace and other similar sites are called ''***social*** media sites''—their purpose is to allow interaction. Indeed, in the first line of his letter to investors that was included in Facebook's initial public offering registration statement, Zuckerberg stated that Facebook ''was built to accomplish a social mission—to make the world more open and connected.''[26] Social media sites are online clubs, not online filing cabinets.

Are There Other Provisions of the SCA that Could Also Apply to Social Media Sites?

Communications on a social media site may still be subject to the SCA, even if those communications are not held in ''electronic storage.'' Section 2702(a)(2) of the SCA prohibits any provider of RCS services to the public from knowingly divulging ''the contents of any communication which is carried or maintained on that

[17] *See* 18 U.S.C. § 2511(2)(g)(i).
[18] *Ehling*, 2013 BL 220816, at *9-*11.
[19] *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 981–82 (C.D. Cal. 2010).
[20] *See Crispin*, 717 F.Supp.2d at 968.
[21] *Id.* at 982.
[22] *Id.* at 989.
[23] *Id.* at 975-976.
[24] *Id.* at 991.
[25] *See* 18 U.S.C. § 2511(g)(i) (''[i]t shall not be unlawful under . . . [the SCA] for any person . . . to intercept or access an electronic communication . . . that . . . is readily accessible to the general public[.]'')
[26] Facebook Inc., Registration Statement (Form, S-1), (Feb. 1, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm.

service.'' Of course, in order to be subject to this provision, a social media site would need to be classified as an RCS provider.

The SCA defines a ''remote computing service'' as ''the provision to the public of computer storage or processing services by means of an electronic communications system[.]''[27] Interestingly, this definition uses the more generic term ''computer storage'' as opposed to ''electronic storage.'' There are of course many services whose fundamental purpose is to provide cloud or Internet-based storage services or computer processing services for other parties (e.g., Amazon Web Services, Google Cloud, Dropbox and Microsoft Office 365).

In contrast with typical cloud service providers, social media sites' core purpose is to provide online social networking services. As a necessary byproduct of those services, they do allow site members to use applications to create and store content to their sites. Therefore, under a strictly literal reading of the SCA (if not perhaps under the reading intended by Congress), social media sites could qualify as RCS providers. And, in fact, the *Crispin* court concluded that Facebook and Myspace were not only ECS providers, but they were also RCS providers as well.[28]

Practical Impact of Ehling and Crispin

The practical impact of *Ehling* and *Crispin* remains to be seen. Both cases were decided by federal trial courts and therefore have nothing more than persuasive value outside of their districts.

There are also other laws that impose more concrete limits on the ability of private parties to obtain access to nonpublic social media web pages. As of Oct. 26, 2013, at least 12 states had passed social media password protection laws that, among other things, limit the ability of employers to request passwords and user names for the purpose of accessing the private social media pages of employees and/or job applicants.[29]

Another existing federal law, the Computer Fraud and Abuse Act (CFAA),[30] broadly prohibits the intentional access of almost any computer without authorization. Accessing protected Web pages of a social media account without authorization could constitute a violation of the CFAA.

Restricting the ability of civil litigants to access private social media content is potentially the most significant outcome of *Ehling* and *Crispin*. If social media sites are deemed to be ECS providers (which would be consistent with the terms of the SCA), and social media content on that site—to the extent protected by a user's privacy settings—is deemed to be in electronic storage (which is perhaps more debatable), then a civil litigant would generally ***not*** be able to obtain such content from the site pursuant to a subpoena. Even if such privacy-protected content is not in electronic storage within the meaning of the SCA, a private litigant would still generally not be able to obtain the content pursuant to subpoena if a court followed *Crispin*'s lead and held that a social media site was an RCS provider.

---

[27] 18 U.S.C. § 2711(2).

[28] *Crispin*, 717 F.Supp.2d at 990.

[29] See *Employer Access to Social Media Usernames and Passwords 2013*, National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last visited Nov. 14, 2013); *Employer Access to Social Media Usernames and Passwords 2012 Legislation*, National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx (last visited Nov. 14, 2013).

[30] 18 U.S.C. § 1030(a)(2).

  ISSN

THIS ARTICLE FIRST APPEARED IN SOCIAL MEDIA LAW & POLICY REPORT

NEW RULES OF ENGAGEMENT

SOCIAL MEDIA LAW & POLICY REPORT

Corporate use of social media is skyrocketing, and so are the legal risks to your clients and their organizations. Now, staying up to date on the latest legal implications just got easier.

Introducing **Social Media Law & Policy Report**™ — the only resource that integrates timely news, real-world analysis, full-text case law, primary sources, reference tools, checklists, and sample policies to help you advise clients with confidence.

START YOUR FREE TRIAL — CALL 800.372.1033
OR GO TO www.bna.com/smlr-article

Bloomberg BNA