THE NATIONAL LAW JOURNAL
MARCH 2019
An ALM Publication

opinion

The Criminal Defense Bar Wants Your Emails

BY JOSHUA LIPSHUTZ AND MICHAEL HOLECEK

BEING THE VICTIM OF A CRIME IS BAD enough. But imagine if being a crime victim also meant the perpetrator could suddenly access all of your private electronic data—your emails, text messages, social-media history and even GPS location history—without your permission or knowledge.

In recent years, criminal defense attorneys have sought to establish a new constitutional "right," grounded in the Fifth and Sixth Amendments, for criminal defendants to access crime victims' and crime witnesses' private electronic communications. Instead of subpoenaing victims and witnesses directly, they are subpoenaing email and social-media service providers to try to obtain the private records of their account holders surreptitiously. And some trial courts are forcing the providers to turn over their users' data.

Fortunately, several recent appellate decisions—including notable ones from the California Supreme Court and D.C. Court of Appeals—have rejected the efforts of criminal defendants, holding that the Stored Communications Act, 18 U.S.C. § 2701, *et seq.* ("SCA"), precludes service providers from disclosing data without their account holders' consent.

In *Facebook, Inc. v. Superior Court (Hunter)*, two defendants charged with a gang-related murder served subpoenas on Facebook, Twitter and other service providers, seeking the private communications of the homicide victim and a prosecution witness. After the trial court declared the subpoenas enforceable, the California Supreme Court held in May 2018 that the SCA prohibits enforcement of the subpoenas.

ANTSTANG/SHUTTERSTOCK.COM

First, the court confirmed that the SCA applies to social-media records maintained by Facebook, Twitter and other providers. The court rejected the defendants' "unsupported and rather startling assertion" that there is "no such thing as true privacy" with social media.

Second, the court held that account holders do not impliedly consent to disclosure by sharing communications on social media, even with a "large group" or friends or followers. Indeed, "a registered user who configures a communication to be viewed by any number of friends or followers—but not by the public generally—evinces an intent

opinion

not to consent to disclosure by a provider …, but instead to preserve some degree of privacy." Thus, although the court refrained from ruling on the constitutionality of the SCA, *Hunter* establishes that the SCA prohibits criminal defendants from obtaining private electronic communications, including social-media communications, without account-holder consent.

In *Facebook, Inc. v. Wint*, decided in January 2019, the D.C. Court of Appeals went even further. On the eve of a criminal defendant's high-profile quadruple-murder trial, the defendant subpoenaed Facebook and Instagram for the social-media records of a prosecution witness, Jordan Wallace. The trial judge denied Facebook's motion to quash the subpoena, finding that the SCA violated the defendant's constitutional due process right to present a complete defense. Remarkably, even though Facebook pointed out that there were dozens of accounts associated with the name Jordan Wallace, the court ordered Facebook to produce to the defendant all of the private records of *anyone* with that name.

The D.C. Court of Appeals reversed. It held that the SCA's prohibition on the disclosure of electronic communications makes no exception for criminal subpoenas. Further, the SCA rationally requires defendants to look to the senders and recipients of electronic communications, instead of third-party service providers: "channeling such discovery to senders and recipients, rather than providers, increases the chance that affected individuals can assert claims of privilege or other rights of privacy before covered communications are disclosed to criminal defendants."

The court also held that a criminal defendant's constitutional right to obtain evidence for his defense is "not unlimited." Because a defendant can subpoena the same evidence from other sources—including message senders and recipients—Wint failed to establish "a serious constitutional doubt" regarding the SCA's prohibitions.

Despite these rulings, the efforts of criminal defendants continue. Later this year, the California Supreme Court will have another opportunity to decide whether the SCA's privacy protections violate the constitutional rights of criminal defendants. In *Facebook, Inc. v. Superior Court (Touchstone)*, the defendant was charged with attempted murder of his sister's boyfriend. Instead of subpoenaing the victim for his social-media records, the defendant subpoenaed Facebook. A California trial court denied Facebook's motion to quash, but, in 2017, the Court of Appeal reversed. Facebook has argued that the SCA prohibits the company from turning over the victim's communications and cannot be unconstitutional because the defendant has other means of obtaining the same evidence—namely, from the victim himself.

The SCA protects the privacy rights of all Americans. With growing frequency, criminal defendants have tried to circumvent and dilute the SCA by subpoenaing private electronic communications from service providers, without account holders' consent. Service providers have gone to great lengths to quash those subpoenas, often engaging in lengthy and costly battles through the appellate courts to protect the privacy of their account holders' communications. Those efforts have had significant success, with several appellate courts recently holding that the SCA's disclosure prohibitions apply to criminal subpoenas and preclude defendants from obtaining private communications without account-holder consent.

Joshua Lipshutz is a partner in the Washington, D.C., and San Francisco offices of Gibson, Dunn & Crutcher. Michael Holecek is a Los Angeles-based Gibson Dunn associate. They represent Facebook and Twitter in the cases described above.