Jennings v. Broome et al.

No. 27177, 2012 S.C. LEXIS 204 (S.C. Oct. 10, 2012)

The Supreme Court of South Carolina ruled in Jennings v. Broome that a private citizen can 'hack' into another person's email account without violating federal law, more specifically the Stored Communications Act, 18 U.S.C. §§ 2701-12.

The public outing of emails about adultery apparently is all the rage these days. Just ask General David Petraeus, who until a few weeks ago was director of the Central Intelligence Agency. He fell from the lofty position once emails between him and his biographer/paramour became public. In that case, the emails became known due to an FBI investigation into suspect emails sent to yet another woman by Petraeus's 'biographer.' Thus, the Petraeus affair was outed by law enforcement officials. However, as a recent case from the Supreme Court of South Carolina shows, a private citizen can 'hack' into another person's email account, access very personal emails, and not run afoul of federal law. The lesson to be learned? Beware the tech savvy daughter-in-law, and do not look to the federal Stored Communications Act, 18 U.S.C. §§ 2701-12, as a means to revenge.

Jennings v. Broome

The story in Jennings v. Broome et al., No. 27177, 2012 S.C. LEXIS 204 (S.C. Oct. 10, 2012) is quite straightforward. Mrs. Jennings believed that her husband was involved in an adulterous affair, and while he did not deny the affair, he would not identify the object of his affections. Mrs. Jennings then confided in her daughter-in-law, Ms. Broome, who used to work for Mr. Jennings, and the daughter-in-law promptly guessed the correct security screen answers to Mr. Jenning's Yahoo! email account and obtained the tell-all emails - copies of which she promptly provided to Mrs. Jennings's divorce attorney and a private investigator. Mr. Jennings then filed suit against the daughter-in-law (as well the divorce attorney and the private investigator) claiming that his email account had been accessed unlawfully under various common law and state law theories, as well as under the federal Stored Communications Act. The trial court granted summary judgment in favour of Ms. Broome and the others, but the state intermediate-level appellate court reversed as to Ms. Broome, finding that her conduct had been unlawful under the federal statute. The case then came up to the South Carolina Supreme Court, which examined the sole question of whether Ms. Broome's actions in accessing Mr. Jennings's Yahoo! account without his authorisation constituted a violation of the federal Stored Communications Act.

In a plurality decision, a group of South Carolina Justices ultimately held that the Stored Communications Act offered Mr. Jennings no relief. In reaching that decision, two of the Justices focused on the plain language of the statue, which provides in relevant part that anyone who 'intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents access to a wire or electronic communication while it is in electronic storage' shall have committed an unlawful act. 18 U.S.C. § 2701(a). Clearly, in this situation, Ms. Boone had intentionally accessed Mr. Jennings's account without authorisation and obtained access to his emails. However, the Court determined that the emails were not in 'electronic storage' within the meaning of the Act.

In recent years, courts have grappled with how to interpret the 'electronic storage' language of the Act, which was adopted in 1986, long before the advent of email. The statutory language is simple enough - i.e., 'electronic storage is defined as (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purpose of backup protection of such communication.' Id. at § 2510(17). First, the South Carolina Court noted that despite the use of the word 'and' between sections (A) and (B), the majority of courts have read the 'and' to be 'or' and have determined that electronic storage can be found where an email is kept by the service provider for purposes of backup regardless even if it is no longer being maintained temporarily as part of the transmission process. Jennings at *6 (citing numerous cases).

The Court then considered what is meant by 'backup' storage. In so doing, the Court specifically rejected the intermediate appellate court's reliance on a 2004 decision from the US Court of Appeals for the Ninth Circuit, Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004), which held that emails that have been opened on an internet service provider's servers, but not downloaded to the person's computer, legitimately could be characterised as being stored for purposes of backup. Jennings at *8. The Jennings Court felt such a reading, however, was too limiting and not consistent with the plain language of the statute. Rather, the Court stated that 'we decline to hold that retaining an opened e-mail constitutes storing it for backup protection' on the grounds that the plain meaning of the word 'backup' as defined by the Merriam-Webster Dictionary is 'one that serves as substitute or support.' Id. Based on this dictionary-based interpretation, the Court went on to explain that Congress's use of the word

'backup' presupposes the existence of another copy of the e-mail which would serve as a substitute or support. Here, there was no other copy and, accordingly, the Court stated that '[w]e see no reason to deviate from the plain, everyday meaning of the word 'backup' and conclude that as the single copy of the communication, Jennings' e-mails could not have been stored for backup protection.' Ibid.

Although concurring in the result, another of the South Carolina Supreme Court Justices, Justice Toal, took issue with the lead opinion on various grounds. Most interestingly, Justice Toal looked at the statutory history of the Act and the difficulty that ensues when trying to apply statutory language to a technology that did not exist at the time the statute was adopted. Specifically, Justice Toal noted that in 1986, when the Act came into being, there was no 'World Wide Web,' or internet as we know it, which arrived in 1990. Id. at *20. Indeed, he explained that in 1986, when Congress passed the Act, electronic mail was described as a communication that was transmitted over telephone lines to another person's computer operated by an electronic mail company - and that person would then have to call the company to retrieve the electronic message from the company's mail box storage, or have the company print out the message and send it via the regular postal system. Id. at * 20-21 (citing S. Rep. No. 99-541 at 7 (1986)). How times have changed!

The EPCA

The extent to which the Stored Communications Act and other provisions of the broader Electronic Communication Privacy Act (ECPA) are outdated has led to very recent efforts to update the text to recognise both the changing technological world in which we now live, as well as evolved concepts of expected privacy rights in electronic communications. For example, in the coming days, the Senate Judiciary Committee is expected to vote on proposed changes to the ECPA to address, among other things, the extent to which law enforcement officials can obtain copies of a person's emails from the internet service provider without a search warrant and without notice to the subscriber. At present, the law requires a search warrant only for emails that are 180 days old or less; older emails can be obtained solely through the use of a subpoena, without a judge's oversight. As a general matter, privacy advocates support the proposed changes, whereas law enforcement groups fear the proposed changes will hamper their ability to track unlawful conduct as shown through email communications.

Until Congress acts, and depending on what changes, if any, are finally adopted, many feel that privacy rights remain at odds with statutory provisions relating to electronic communications. This means that, at least for now, Mr. Jennings and others like him cannot necessarily depend on federal law or the courts to protect their personal emails from prying eyes - whether those eyes belong to law enforcement personnel or a clever daughter-in-law.

Melinda Levitt Partner
Foley & Lardner LLP
MLevitt@foley.com