

New Jersey Law Journal

VOL. CXC—NO. 10—INDEX 891

DECEMBER 3, 2007

ESTABLISHED 1878

Commentary

E-Mail Users Expect Privacy, and Deserve It

By Grayson Barber

When Charles Katz entered a glass telephone booth in downtown Los Angeles to call his bookie, did he have an expectation of privacy? The year was 1965, and the law of the land was the “trespass” doctrine of *Olmstead v. United States*, 277 U.S. 438 (1928). For decades, the police had been free to tap phones without search warrants.

According to the U.S. Supreme Court, *Katz* did create an expectation of privacy — by closing the glass door of the phone booth. “The Fourth Amendment protects people, not places,” it ruled. Since then, the police have had to obtain search warrants in order to tap conventional telephone communications. The Court recognized, it seemed, the wisdom of Justice Louis Brandeis, whose dissent in *Olmstead* characterized privacy as the “right to be left alone.”

But times have changed. On the Internet, when can one reasonably expect to be left alone? Surfing the Internet to visit legal Web sites? Using e-mail to plan a lunch date? Storing family photos on Internet sites like Flickr?

Many lawyers will invoke *Katz v. United States*, 389 U.S. 347 (1967), for the proposition that on the Internet you

have no “reasonable expectation of privacy.” This phrase comes not from the Court’s decision in *Katz*, but from Justice John Marshall Harlan II’s concurring opinion. Like “clear and present danger,” it sticks in the mind, even though it represents an incomplete statement of the law.

By decoupling privacy expectations from the old doctrine of trespass, the *Katz* decision should have expanded the scope of Fourth Amendment protection. Instead, the “reasonable expectation” test has been used to suggest we relinquish all privacy the moment we cross the doorsteps of our homes.

Moreover, significant U.S. Supreme Court cases in the 1970s ruled that individuals have no protected privacy interest in records voluntarily disclosed to businesses. Once you disclose personal records to a third party, the information enjoys no Fourth Amendment protection, the Court held in *United States v. Miller*, 425 U.S. 435 (1976) (bank records), and *Smith v. Maryland*, 442 U.S. 735 (1979) (phone records).

The third-party doctrine raises the possibility that electronic files, unintentionally placed on remote commercial servers for safekeeping, are wholly without Fourth Amendment protection. This proposition, broadly supported by the law enforcement community, does

not match the ordinary expectations of ordinary computer users, who often make intimate disclosures thinking they are anonymous online.

Congress stepped in to cure, or at least clarify, expectations in 1986. The Electronic Communications Privacy Act (ECPA) offered privacy in the form of limitations on government power, and protections against commercial exploitation of personal data. But in 1986, more than 20 years ago, few people used e-mail or the Internet, and the World Wide Web did not yet exist.

The electronic surveillance laws created by ECPA comprise three statutes: the Wiretap Act, the Pen Register Statute and the Stored Communications Act.

As applied to e-mail, each of these statutes provides different levels of protection, depending on the duration and location of storage and on whether the e-mail has been opened. This can become very convoluted. As data flow from sender to recipient, the content of electronic communication is handled by a series of routers that are owned by many different entities. As communications traverse the network, they leave replicas of themselves, in whole or in pieces, in the hands of any number of third parties.

The Supreme Court has not considered whether individuals have a reasonable expectation of privacy in their e-mail. Deirdre Mulligan, a law professor at the University of California at Berkeley, argues they should. In a persuasive law review article, “Reasonable Expectations in

Barber, a solo in Princeton, concentrates on privacy matters. In State v. Reid, she represents amici curiae the ACLU-NJ, the Electronic Frontier Foundation, the Electronic Privacy Information Center, the New Jersey Library Association, the Freedom to Read Foundation and the Privacy Rights Clearinghouse.

Electronic Communications: A Critical Perspective on ECPA,” 72 *Geo. Wash. L. Rev.* 1557 (2004), she points out that unlike the third-party businesses at issue in *Miller* and *Smith*, Internet Service Providers are “mere conduits” for information.

A related question is pending before the New Jersey Supreme Court in *State v. Reid*, No. 60-756. Although the *Reid* case does not concern e-mail, it asks whether the police should be

limited in their power to obtain information about anonymous computer users.

The U.S. Supreme Court developed the third-party doctrine in cases where banks and phone companies, for example, were not conduits, but had separate and independent interests in the information and transactions. Sending an e-mail through the pipeline of an ISP does not involve the same kind of voluntary disclosure.

For this reason, electronic communications deserve stronger Fourth Amendment protection than other types of third-party disclosures. Justice Brandeis was truly prescient when he observed, “Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.” ■